Safer (Cyber)Spaces

Reconfiguring Digital Security Towards Solidarity

Julia Słupska

Oxford Internet Institute

Centre for Doctoral Training in Cybersecurity

University of Oxford

Michaelmas 2022

Thesis submitted in partial fulfilment of the requirements for the degree of DPhil in Cybersecurity in the Oxford Internet Institute at the University of Oxford

Word Count: 65,834

Table of Contents

Abstract

As technology increasingly mediates our relationships, it also enables existing patterns of coercion, abuse, and control. This thesis investigates digital safety and security in the context of intimate violence and coercive control. I first develop a feminist critique of cybersecurity: namely, that due to the discipline's engineering focus on defending networks and information, cybersecurity neglects the human element, and particularly differences in power and relationships between humans that produce (in)security. Feminist and critical theories, which centre gender and power in interpersonal relationships, provide a useful corrective to this highly masculinised and avowedly apolitical field. Taking this critique as a starting point, I present a set of studies that answer the overarching research question: *"how can we reconfigure cybersecurity to account for tech-facilitated coercive control?"* I focus on responses to the phenomenon of technology-enabled coercive control, or 'tech abuse' as a site for examining alternative security practices.

I then present three studies that reconfigure cybersecurity through running participatory workshops with excluded and marginalised groups, interviewing advocates who support survivors of technology abuse and addressing intimate violence in cybersecurity design. The model of cybersecurity that emerges from these studies is relational, made up of communal 'networks of care' rather than devices and individuals. This carries weight for questions of epistemology and academic knowledge production; my work centres the knowledge of unconventional and unacknowledged experts, such as survivors of abuse and community practitioners who support them. These people are cybersecurity experts due to their on-the-ground understanding of how technology is co-opted for abuse. Security practitioners should recognise the expertise inherent in these care networks to build on and strengthen them with a mindset of solidarity rather than turning these social problems into opportunities to pitch new technical products. Cybersecurity which starts with people (not machines), especially marginalised people, points our attention to dismantling the broader structures that create insecurity rather than patching technical vulnerabilities. In doing so, this reconfigured security becomes a call for solidarity.

Acknowledgements

This thesis would not have been possible without many different sources of support and inspiration, for which I am immensely grateful. Thank you first to my supervisors, Gina, Helena and Joss for their valuable encouragement and feedback. This work was made possible and aided immensely by a ESPSRC Cybersecurity Studentship grant and a UK Research & Innovation Citizen Science grant.

Thank you to all my incredible collaborators, particularly Leonie, Angelika, Toby and Megan, from whom I learned so much. Thank you especially to Scarlet, for the countless hours of work, ideas, and laughter without which re:configure would never have been possible, and certainly not for so many months longer than we expected. Thank you to Nayana, Selina, Inda, Hubert, and all others who volunteered in the re:configure project. Thank you to James for reading an earlier draft of this thesis and for very insightful comments. Thank you to Laura for all our conversations exploring feminist cybersecurity, it was such a delight to twin our PhDs. Thank you also to Lizzie and the members of the Royal Holloway Critical Security Reading group for helping me wrap my head around critical security. My research and thinking benefitted enormously from working alongside activists and organisers working on technology justice: thank you in particular to the San Diego Tech Workers Coalition and No Tech for Tyrants.

Thank you to my mum for my work ethic and my dad for my contrarianism. Thank you to Sister Mary for pointing me towards the notion of solidarity and for your incredible kindness. Thank you to Jeremy and Ellen for being the greatest. Thank you to Jaś and Julia my beloved niblings Zosia, Michał, Xavek and Tadam for keeping me sane via Skype during the long lockdown.

Thank you to all my housemates, especially Patrick, Gaspard, Nayana, Yung, Calvin and Cailean, for helping make Henley such a special home for me. Thank you to Nancy, Yung and Sruj for always reminding me of the importance of rest and critical thinking. Thank you to Karolina for the most interesting conversations. Thank you to Adam for reminding me people get into STEM to build better worlds, to Ben for never-ending care work, Hattie, Hailey, David, Kenneth, Wyn and all the other inhabitants of Stardust Motel for their incredible hospitality. Thank you to Dani (for keeping me afloat), Amy (for being a sex positivity icon) and Paula (for the quiet anarchy of communal soup), and for all your wisdom, kindness, and support.

Last but not least, thank you to all the participants in this research, who contributed their time, energy and ideas, and whose advocacy and experiences continue to inspire me. In particular, thank you so much to Mallika and Marissa and all the members of Voice of Domestic Workers for the crucial and difficult work you do.

"Feminism is not a philosophy, or a theory, or even a point of view. It is a political movement to transform the world beyond recognition. It asks: what would it be to end the political, social, sexual, economic, psychological, and physical subordination of women? It answers: we do not know; let us try to see."

- *Amia Srinivasan, The Right to Sex*

Chapter 1: Introduction

The Maid and the Businessman

Whose security is cybersecurity? A cybersecurity threat model is a stylised representation of a scenario in which the security of a technical system is compromised by an attacker. As with any abstraction, it carries assumptions about the nature of the attacker, the system to be protected, and what kinds of solutions might be implemented. These assumptions in turn reflect the social standpoint and positionality of security practitioners and researchers.

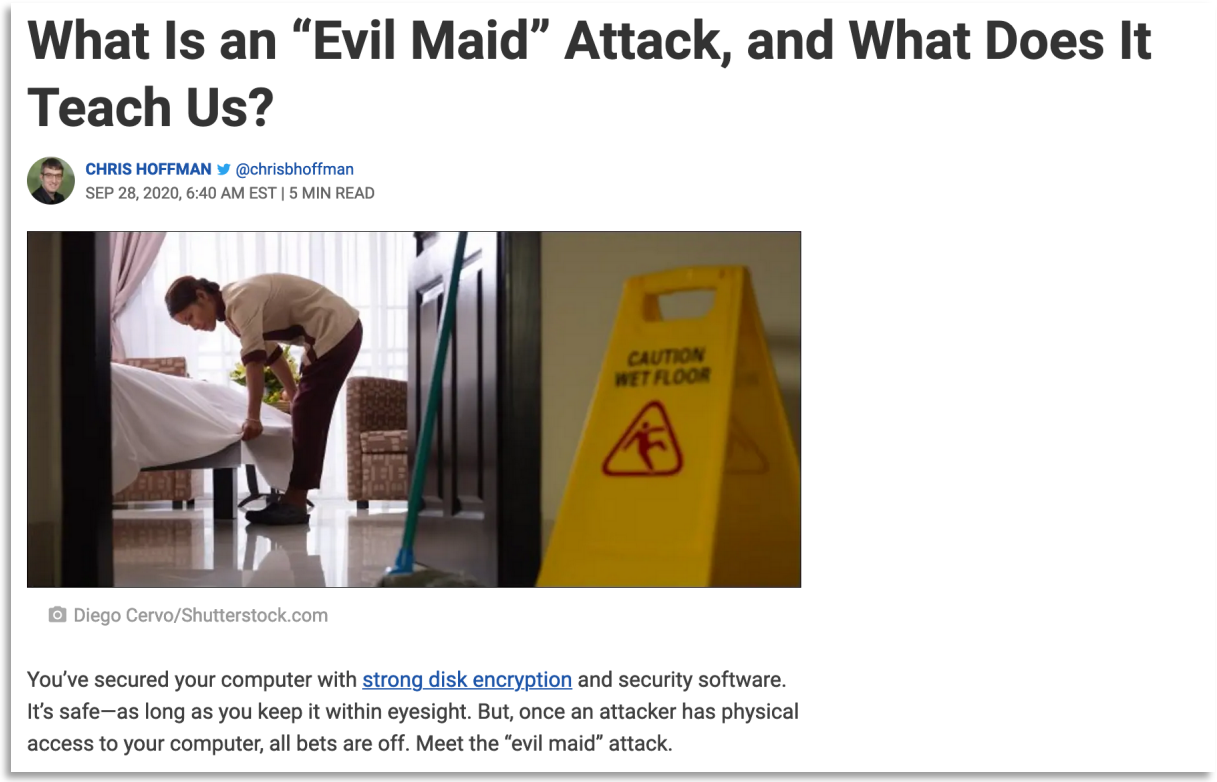

Figure 1: screenshot from blogpost on “Evil Maid” attack

Consider the “evil maid attack”, a cybersecurity threat model in which a travelling businessman leaves his laptop in his hotel room (see Figure 1). In this model, a hotel maid compromises the unattended device using, for example, a USB flash drive. When the businessman returns to his laptop, he enters his password into a fake password prompt, which sends his password to the attacker. Armed with the stolen password, the maid returns to the room the next time the businessman leaves and steals the data from his laptop. Many information security researchers and professionals have worked on the evil maid attack through, for example, identifying and mitigating hardware and software vulnerabilities in devices and developing security protocols to defend against physical compromise (Tereshkin, 2010).

Yet how often has a hotel maid been a threat to a businessman's security, and vice versa? Given the high rates of sexual and other forms of harassment against workers in the hospitality industry (who are often employed on precarious labour contracts with little protection), it seems improbable to fixate on a model of the maid as a threat. Why is there a body of cybersecurity literature defending the businessman, but not the maid? Although "evil maid"-type attacks have been documented, these cases are treated as newsworthy because they are exceptional (whereas routine harassment of hospitality workers is hardly a news story).

Many in the field may respond that cybersecurity exists to defend devices and systems, not to engage in political questions such as sexual harassment. Yet devices and systems always belong to someone. The prevalence of imagery such as the "evil maid" points to a systematic defence of those who, like company executives or government officials, have the wealth and power to purchase and develop computer systems. This is particularly true given the lack of focus on threats faced by domestic workers, such as pervasive CCTV surveillance. Domestic workers, like many other marginalised groups, are instead either ignored or treated as a threat in security research.

Security and Power

A far more likely scenario in which an attacker has repeat physical access to a device is the threat model of intimate partner violence, in which an abusive current or former partner or family member uses technology to coerce or control someone in their intimate circle. Yet these kinds of technology-enabled coercive control (shortened to 'tech abuse' in this thesis), a form of violence which disproportionately affects women and marginalised people, historically were not considered in cybersecurity research (Slupska 2019).

This is a serious failure, as intimate abuse is much more common than is widely understood. A UN study on global homicide rates found that worldwide, women were more likely to be killed at home than anywhere else, with 58% of all female victims of homicide murdered by intimate partners or family members (UNODC, 2018). Each year, abuse and coercive control make millions of people vulnerable worldwide, particularly people who are members of marginalised groups (Devries et al., 2013; Sokoloff & Dupont, 2005). I use the terms 'marginalised people' and 'marginalised groups' to indicate people who are made marginal by discrimination or oppression based on gender, race, disability, class, caste, age, nationality, language, location or other "hierarchies of difference", and usually due to multiple factors in combination (Collins, 1990).

Similarly to the term 'minoritized,' the term 'marginalised' is useful because it indicates that no one is inherently vulnerable or marginal. Instead, people are *made marginal* by processes of

power and domination. These processes can be political (such as the law or law enforcement), economic (income inequality) or social (various forms of prejudice). In this sense, violence, and abuse both disproportionately affect marginalised groups, and are part of the processes of marginalisation.

Arguments such as the one about the evil maid threat model draw on feminist standpoint epistemology, which notes how a person's social standpoint, or positionality, shapes their knowledge of the world (Collins, 1990; Harding, 2016). A threat model, as a form of knowledge, reflects the particular social standpoint of the security researcher who imagines it into being. Marginalized groups are socially situated in ways that make it more possible for them to be aware of dynamics such as oppressive structures than it is for the non-marginalized. Many feminist theorists have developed methods for centring marginalised peoples' perspectives in research (Crenshaw, 1989; Harding, 2001; hooks, 1984). In particular, hooks (1984) advocates for including the knowledge and awareness of the lives of women and men who live in the margin in feminist theory. My work responds to this call by using participatory methods to centre perspectives which were traditionally excluded from (cyber)security research. I introduce a feminist critique and reconfiguring of cybersecurity, arguing it should be grounded by a focus on harms to *people* (particularly marginalised people) rather than *devices or systems* (Slupska, 2019; Slupska et al., 2021).

I focus on the phenomenon of technology-enabled coercive control, or 'tech abuse' as a case study for examining security practices outside the conventional arena of military and corporate security. Studying digital security in this context allows me to explore a series of questions about the nature of security in a technology-mediated social world. How does responding to problems like tech abuse change how we should understand security? Can security, a paradigm developed to defend militaries and businesses, be reconfigured to defend marginalised people (in other words, to defend the maid and not the businessman)? Echoing Srinivasan's (2022) question of what would it be to end the subjugation of women, I ask: what would a feminist cybersecurity be like? I distil these broad questions into one overarching research question (ORQ): *"How can we reconfigure cybersecurity practices to account for technology-enabled coercive control?"* For clarity, I break down this overarching research question into three sub research questions:

- RQ1: Why do existing security practices fail to account for technology-mediated coercive control?
- RQ2: How can we use feminist epistemology and participatory methods to reconfigure security practices?
- RQ3: Should we reconfigure cybersecurity practices to account for technology-enabled coercive control?

To answer these questions, I draw on critical and feminist theories, in particular their critiques of security, alternative approaches to safety, and research methodologies. By applying these theories and methods to (cyber)security, I examine whether it is possible for this framework to challenge rather than reinforce structural forms of power and oppression. The following section explains how my methods and studies answer my research question.

Research questions and chapter structure

Throughout my three studies, I answer my overarching research question (ORQ) both by developing new methods and studying existing practices in the field of coercive control. Each chapter offers a different perspective on how we can and should respond to tech abuse, as well as the broader implications of reconfiguring online safety and security to account for power relations.

In Chapter 2, I develop a literature review and conceptual framework. I examine the concept of security, as well as critiques of security from the overlapping but distinct fields of critical security studies, critical race theory, and feminist theories. While these theories are varied and sometimes disagree on how to approach security problems, they all share an analytical focus on critiquing power and how power can shape academic knowledge production. Therefore, I review these literatures with a focus on RQ1: "*Why do existing security practices fail to account for technology-mediated coercive control?*" Critical security theorists are sceptical of redeeming the concept of security, arguing it justifies authoritarian tendencies and entrenches discrimination along racial lines as well as other forms of marginalisation. In contrast, some feminist theories (although also critical of security as masculinised and wilfully ignorant of gendered problems like intimate partner violence) see avenues for a reconfigured feminist security which draws on notions like ethics of care and safer spaces to defend marginalised people. This aspiration for a reconfigured, feminist security motivates RQ2. Less attention has been paid to exploring what security already looks like when it is applied to address feminist concerns and defend marginalised people. This thesis contributes to this gap both by developing and examining a variety of potential feminist approaches to cybersecurity, particularly through addressing problems like coercive control. Consequently, this chapter also defines the concept of technology-enabled coercive control and reviews existing literature on it, as well as outlining my methodology .

In Chapter 3, I conduct a review of smart home security analysis papers to show how the threat model of intimate partner violence is almost entirely absent in the literature. This contributes to my theoretical critique of security and further develops my answer to RQ1. Having established

that conventional cybersecurity threat models omit tech abuse, I then develop a threat model for intimate partner and family violence adapting Shostack's (2014) method of threat modelling. Lastly, I note limitations in this expanded approach, outlining how these changes open space for further problematisation of threat modelling.

In Chapter 4, I present a methodological innovation which applies feminist participatory action research methods to the cybersecurity method of threat modelling, I describe two studies which invite "non-experts" (such as migrant domestic workers, activists, and members of the general public) to define their own threats in a process of *participatory threat modelling (PTM).* PTM is my response to the research question RQ2: "*How can we use feminist epistemology and participatory methods to reconfigure security practices?"* Developing and improving this method through a series of 12 workshops with various community groups forms one of the major contributions of my thesis. This method allows security research to incorporate power imbalances and centre marginalised peoples' experiences. By asking participants to define their own threats, my research collaborators and I developed more robust threat models which included structural factors which create insecurity. This results in an expanded understanding of tech-facilitated coercive control, as a form of abuse perpetrated not only by intimate partners, but also by employers and state actors. This also allowed us to map how different forms of threat reinforce each other (such as the way insecure immigration status can make migrant domestic workers vulnerable to online scams and harassment). Therefore, this method offers a clear foundation for reconfiguring cybersecurity to account for abuse and power relations.

In Chapter 5, I present the results of 26 interviews with advocates who support survivors of tech abuse. This study further develops my answer to RQ2, by drawing on critiques of expertise grounded in feminist epistemology. By looking at the context of responses to intimate partner violence and coercive control, I present a study of security practices defending marginalised people. I outline how these security practices are made up of intertwined psychological and technical support and introduce the idea of "networks of care": networks of practitioners who support those who have experienced gender-based violence and tech abuse, usually beyond the state. Building on the findings of Chapter 4, I argue for community and care-based forms of security as a positive alternative to carceral state or corporate security.

In Chapter 6, I return to my overarching research question (ORQ) and make recommendations for how researchers and practitioners can incorporate 'abusability' into various stages of the product design lifecycle, drawing on the design recommendations of tech abuse practitioners. In doing so, I explore the benefits and limitations of using conventional cybersecurity methods to address this problem and offer pragmatic recommendations for cybersecurity practices which

not only account for but can even counteract oppressive power relations. I also develop a maturity model for abusability, which can be used to evaluate company practices and support accountability mechanisms.

Finally, in Chapter 7, I conclude with a summary of my findings and contributions. To address tech-facilitated coercive control—both in its interpersonal and structural forms—we must reconfigure both the conceptual underpinning and the practices of cybersecurity. This includes acknowledging how intersecting power relations create insecurity, rejecting the mindset of surveillance-driven security and technological solutionism, and investing instead in supporting the expertise and security practices already existing in community support groups and networks. Therefore, this thesis is a call to reconfigure cybersecurity towards solidarity.

Table 1: Research questions and methods

Overarching research question (**ORQ**): How can we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

- RQ1: Why do existing security practices fail to account for technology-mediated coercive control?
- RQ2: How can we use feminist epistemology and participatory methods to reconfigure security practices?
- RQ3: Should we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

Chapter	**RQ**	**Method & data**	**Contributions**
Chapter 2: Conceptual framework	RQ1, RQ2	Literature review	Theoretical: by drawing on feminist methods and shifting focus from security to safety, security research can counterbalance power dynamics.
Chapter 3: Threat modelling intimate partner violence	RQ1	Threat modelling	Empirical: demonstrates gap in security analysis literature Methodological: threat model for IPV
Chapter 4: Feminist action research	RQ2	Workshops in partnership with community orgs, interviews	Methodological: participatory threat modelling Theoretical: TM with marginalised people points to community support networks & structural insecurity rather than technical vulnerabilities
Chapter 5: Networks of care	RQ2	Interviews	Empirical: security made of intertwined technical & emotional support practices Theoretical: networks of care as source of security, nature of expertise
Chapter 6: Abusability	ORQ, RQ3	Literature review, interviews, workshop	Pragmatic/methodological: recommendation for altering threat modelling & building more responsive systems

Chapter 7: Conclusion: From Security to Solidarity	ORQ	N/a	Synthesises and summarises contributions and overall thesis argument

Through critiquing, experimenting with and ultimately reconfiguring various cybersecurity concepts and practices, such as threat modelling and technical expertise, I offer a new approach to (cyber)security, which will be relevant to a wide variety of researchers and practitioners in the intertwined fields of technology, security, and gender-based violence. The following chapter outlines the conceptual framework and theoretical traditions which open up these alternative ways of understanding cybersecurity.

Chapter 2: Towards a Feminist Cybersecurity?

Feminist theory provides compelling ways to critique cybersecurity. Cybersecurity sits at the intersection of technology and security: two fields strongly associated with modern, White Western masculinity (Oldenziel, 1999; Tickner, 2004a). As an industry, it is also disproportionately male, with only 24% of the global cybersecurity workforce identifying as women (ISC, 2017). Focused primarily on spheres coded as "masculine", such as the military or corporate worlds, cybersecurity research and practice also neglects spheres coded as "feminine" such as the domestic (Slupska 2019). This is evident in how cybersecurity threat models do not consider a current or former partner to be a likely source of threat (discussed further in Chapter 3).

Feminist theories, which centre gender and power in intimate or personal relationships, can provide a useful corrective to the highly masculinised and often avowedly apolitical field of cybersecurity. Yet many theorists see security as an inherently oppressive concept. It is important for us not to assume that a feminist cybersecurity is desirable, or even possible. Can a feminist security counterbalance unjust power dynamics? What would it mean for (cyber)security to be feminist?

To answer these questions, I first set out a working definition of cybersecurity in section 1. I then I flesh out this feminist critique of security and situate it within broader critiques of security within critical security studies, critical race theory, and feminist security studies. While much attention has been paid to critiquing security and debates as to whether security should be rejected or reformulated, there is relatively little research empirically documenting security practices in alternative and potentially more empowering sites. In section 2, I explain why feminist theory offers not only a critique of security, but a potentially fruitful source of alternative approaches to cybersecurity, rooted in notions of care, solidarity, and participatory methodology. Although feminism is not a panacea, it offers a useful framework for making safer (cyber)spaces. Taking this focus of reconfiguring (cyber)security to centre marginalised people (rather than rejecting it altogether) can provide a means to work within and improve existing frameworks which are familiar to those who design and develop technology. In section 3, I expand on how critical and feminist methodologies inform my approach to methodology, encapsulated in the notion of reconfiguring. I reflect on my positionality, limitations, and the risks of co-option in this search for a feminist cybersecurity. Critics of white feminism have noted the ways that feminism can be co-opted by capitalism and the carceral state: this could easily be true for a feminist cybersecurity as well.

Lastly, in section 4, I introduce the primary case study of this thesis: technology-enabled abuse, which has been understood as a form of GBV, and therefore within the classic remit of feminist activism and scholarship. Through exploring responses to tech abuse, I seek to incorporate and build upon these theoretical critiques and possible alternatives to security.

(Cyber)security

Defining (cyber)security

Academic research on cybersecurity field is rife with debate over the terms "information security," "cybersecurity", "computer security," "data security" or "digital security" (not to mention "cyber-security" or "cyber security") (Floridi, 2005; Nissenbaum, 2005; Solms & Niekerk, 2013; Veale & Brown, 2020). To understand these debates, it is helpful to first establish a working definition of security.

One way to understand security is as a state of being; for example, the "state of being free from danger and threat" (Shepherd & Weldes, 2008). In this sense, a *referent object* (such as a person, an institution, or an object like a device or computer system) is either secure (free from threat) or insecure (compromised by a threat). For example, in the case of state security, one might say the state (the referent object) is insecure due to external threats from aggressive neighbours or internal threats such as groups categorised as terrorist organisations.

Another way to understand security, favoured by many theorists in the tradition of security studies, is as a set of practices, i.e., the customary or habitual ways of doing something or implementing an idea (Aradau et al., 2014; Bueger, 2016). In the example above, security would then be used to describe the practices the state undertakes to secure itself, such as funding a standing military, developing new weapons, or categorising certain actors as criminals or terrorists to take actions such as surveillance or detention. Common cybersecurity practices can include threat modelling, malware analysis, or red teaming.

Returning now to the concept of cybersecurity, we can see many of the discussions over the rightful definition of the term are related to disagreements over the "referent object", i.e., who or what should be protected. Early understandings of 'information security' such as the classic 'CIA triad,' focused on securing *information.* The CIA triad closely encapsulates the understanding of security (described above) as a state of being. This definition of information security presents security as made up of three properties of information or systems:

- Confidentiality (information should not be shared with unauthorised parties)
- Integrity (information should not be altered in a way that disrupts its accuracy, consistency, or trustworthiness)
- Availability (information should be accessible)

These three properties, collectively called the "CIA triad" have been the basis of information security since the late 1970s (A. J. Neumann, 1977; Veale & Brown, 2020).

Later definitions of "computer" or "cyber" security focus on defending computer systems and networks rather than the more abstract "information." For example, Kello (2017) defines cybersecurity as "measures to protect cyberspace from hostile action," where "cyberspace" is defined as "all computer systems and networks in existence." Similarly, the widely used International Telecommunication Union (ITU) definition (ITU-T, 2008) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." Notably, these definitions focus on computer systems and networks as "assets" in a way that inevitably limits focus to property.

Others, such as Von Solms and Van Niekerk (2013), argue cybersecurity goes beyond information security, as the term encompasses not just the protection of information, machines, or networks, but also the protection of "other assets, including people, which need to be protected due to vulnerabilities that exist as a result of the use of information and communication technologies (ICTs)." They argue this explains the inclusion of misinformation and cyberbullying in national cybersecurity strategies. This understanding of cybersecurity expands the property-oriented frame of cybersecurity by including "people" in the category of "assets." Floridi (2005) takes a somewhat similar approach, through an ontological interpretation of individual people as being constituted by their information and, therefore, understanding a breach of one's informational privacy as a form of aggression towards one's personal identity.

Moving away from defining security as a state of being and seeing it instead as a practice is a constructive way to navigate this debate. Problem definition can itself be seen as a cybersecurity practice: many have argued that *in practice*, cybersecurity defines concerns too narrowly (Coles-Kemp et al., 2018b; Deibert, 2018; von Solms & van Niekerk, 2013). Veale and Brown (2020) critique the term "cybersecurity" for its strong association with national security and defence agencies (as opposed to individual civilian humans). Several subfields—human factors in security or usable privacy and security—broaden this focus by examining psychological and behavioural factors which shape information security, such as the reasons employees press phishing links (Dhamija et al., 2006) or usability difficulties in encrypting email (Whitten & Tygar, 1999a). Much of this research positions humans and human behaviour

as an obstacle that information security needs to overcome, pithily summarised in a common joke in the field: "the biggest security vulnerability is the link between keyboard and chair." Even critiques of this literature which advocate towards a move from "humans-as-a-problem" to "humans-as-a-solution" implicitly cast the information system (or, at times, the organisation which owns them), rather than the humans using it, as the referent object of security (Zimmermann & Renaud, 2019).

Coles-Kemp et al. (2018) develop the concept of a "post-digital" society in which the use of digital technology in everyday life has become inseparable from wider social and cultural practices. Drawing on Cramer's (2015) argument that digital technology has become so intrinsically interwoven into the fabrics of societies and into people's daily lives that "digital" no longer makes sense as a standalone concept, Coles-Kemp et al (2020) propose a "post-digital" security in which people's security concerns are addressed through a combination of human relations and trust as well as technological security mechanisms. Although I do not use the term "post-digital security" (as I find it can be somewhat confusing), I adopt this approach to cybersecurity in my thesis. As I argue throughout my work (Slupska, 2019; Slupska et al., 2021), a feminist approach to cybersecurity must be grounded by a focus on harms to *people* (particularly marginalised people) rather than *devices or systems*. Therefore, when I refer to cybersecurity, I mean "the collection of practices, concepts and tools assembled to protect people from technologically-mediated threats." With this definition in mind, I return to the broader debates around whether security is inherently oppressive within critical security studies, critical race theory, and feminist security studies.

Critiques of security

Theorists writing in the traditions of critical security studies, critical race theory, prison abolition, and feminist security studies all share a deep scepticism of the role that the concept of security plays in propping up authoritarianism, racism, and other forms of oppression. Therefore, many critical theorists advocate for moving away from the notion of security entirely, favouring values like emancipation or human flourishing instead.

Critical theorists often illustrate or deconstruct how ideas about security, as well as practices in which those ideas are enacted, lead to harmful outcomes (Doty, 2007; Dwyer et al., 2022; Neocleous, 2003; Nissenbaum, 2005). Common security practices include surveillance or predictive policing as well as discursive practices like securitisation, i.e., framing a policy area (like the "war on drugs" or immigration) as a security issue (Doty, 2007). Securitisation involves naming something or someone as a threat and recommending measures (usually undertaken by state actors such as the police or military) that must be implemented to counter or mitigate the

threat leads. Critical security theorists are generally sceptical of this process (or 'logic') of securitisation, arguing it is used to justify imposing and extending carceral or authoritarian state power (Neocleous, 2003), as well as technologies that are abusive or cement problematic power relationships (Stahl et al., 2014). For example, many critical security and human rights theorists argue that security laws in the aftermath of terrorist acts (such as the Patriot Act after 9/11) undermine civil liberties and lead to a rise in authoritarianism. This is evident in the ways that "national security" is often cited as an exemption from various rights regimes such as the right to privacy or even the right to fair trial (Nissenbaum, 2005). Security intellectuals in academia and think tanks reinforce and profit from these logics of securitisation, benefitting from the status of "expert" on various security subjects (Neocleous, 2003).

Smith (2005) elaborates this logic of security by defining two subcomponents, or building blocks, of security: (1) values (which shape and define the order); and (2) a membership (who subscribe to those values). In this view, security processes include specific measures of security that control the members of an order. The identification of security threats reinforces certain persons and structures of the order (such as law enforcement or the military) as being the definers of the order. Finally, that the implementation of certain security measures can change and transform the order itself (Smith, 2005).

Technology theorists writing in the tradition of critical race studies, such as Browne (2015), Benjamin (2019) and Petty (2019) highlight how security technologies embed a carceral logic that upholds white supremacy through surveillance and criminalisation of raced bodies. Browne (2015) shows how contemporary surveillance technologies are informed by long histories of racist policing, such as branding, runaway slave notices, and lantern laws. Alongside other critical surveillance theorists, she demonstrates how surveillance inherently reifies boundaries, borders, and bodies around racial lines. Carceral logics can also apply to domains outside of the military and policing. Benjamin et al (2019) trace how carceral logics are re-enacted in technology used in settings as various as supermarkets and workplace surveillance. Similarly, Stahl et al. (2014) document how access control settings in a hospital computer system cement a hierarchical relationship between patients and doctors that is at odds with the hospital's patient-centred values.

Petty (2019), writing as a part of the Our Data Bodies collective, critiques the way "security" is equated with "safety." She argues security is primarily about securing items, property, or identity, and often does not have a human factor involved. This kind of security can be at odds with people's safety, particularly people who are marginalised:

> "Often, for undocumented, Black communities and other marginalized communities, the more secure a city proposes to be, the less safe those communities become. When cities invest in the security of neighbourhoods by adding surveillance cameras and increasing the militarization of police departments, it poses an imminent threat to those residents who are often deemed expendable. The security mindset without the human element is inherently unsafe."

Petty argues safety is increased by nurturing relationships and providing adequate resources for health and mental health rather than building security systems.

18 January | Blog | Kim M Reynolds

SAFETY VS. SECURITY: ARE YOU SAFE OR ARE YOU SECURE?

By Tawana Petty

Figure 2: Screenshot of 'safety' mind map from Our Data Bodies blog

Others propose notions of "human security" (Doty, 2007; Kaldor, 2007), "people-centred security" (Coles-Kemp et al. 2018) or "positive security" (Roe, 2008)—i.e., the "defence of just

values" as an alternative to state-centric, carceral, or "negative", threat-based notions of security. Some feminist theorists see potential for reconfiguring security as opposed to just rejecting it (I will return to these possibilities in the section on feminism below). As Doty (2007) notes, formulations such as human security have been criticised as idealistic, or "as everything and nothing" by scholars who at times "seem more interested in the coherence and legitimacy of security studies as an academic field than in the real world of human beings whose lives are affected by the issues that [they want] to exclude from the agenda."

Many theorists writing on this subject agree that collective action, co-operation, and community responses are necessary to address security/safety concerns, but they differ in how they use the term security. Both approaches also seek to dismantle many forms of oppressive, state-centric, or techno-authoritarian forms of security. The difference therefore lies primarily in how different scholars use the term "security." Coles-Kemp et al (2020) as well as other authors they identify as a part of "post-digital security scholarship" attempt to reconfigure security as a concept that is more people-centred. As Dwyer et al. (2022) note, this allows them to maintain relevance and access to mainstream "security" conversation." In contrast, Petty (2019) distinguishes security from safety to critique how technology- and property-centred "security" is, and therefore represents a more radical positioning of these arguments. Emerging approaches to critical cybersecurity aim to "undo cybersecurity in ways that can reassess and challenge power structures in the twenty-first century" (Dwyer et al., 2022).

Abolitionist theorists have warned of a tendency towards "reformist reforms": i.e., measures which purport to reform an abusive system but end up materially and ideologically reinforcing the status quo of the system they are supposedly critiquing (Gorz, 1967). For example, reforms such as mandated police bodycams, which are meant to create accountability for abusive policing, transfer significant technology and resources to police departments, are easily turned off and therefore fail to support accountability, enhance police officers' surveillance capabilities, and deliver a public relations win which can remove steam from more wide-ranging reforms (Dubler & Lloyd, 2019). There is a risk that a move towards feminist cybersecurity would similarly add a socially acceptable gloss to an otherwise functionally oppressive discipline.

My work is shaped by this tension between a desire to formulate a positive security and to reject the concept altogether, as I see merits in both approaches. As a result, I alternate between using safety and security throughout the thesis. When I refer to security, I use the more sociological understanding of security as practice rather than a state of being. I focus on examining security practices rather than defining what exactly it might mean to be "safe" or "secure" online, or rather, I believe it is necessary to focus on the former to define the latter.

While much attention has been paid to critiquing harmful security practices and debating whether security can be reformed to be more positive and less oppressive, less attention has been paid to exploring what digital or cyber- security looks like when it does try to address these more human or people-centred concerns (Dwyer et al., 2022). My thesis responds to this gap through empirically studying sites in which positive security practices may be found and reconfiguring various security practices using feminist methods. Before I expand on this notion of reconfiguring, I will first outline what I mean by 'a feminist approach' and why a feminist approach might be helpful in this situation.

Feminist alternatives

I see my research as a part of a broad feminist political project which seeks to "eradicate the ideology of domination that permeates Western culture" (hooks 1984: 18). My thesis draws on feminist scholarship in its theoretical framework, methodology, and activist orientation. Feminist theory and scholarship emerged from feminist activism, and therefore is to some extent impossible to distinguish from feminist activism and ideology more broadly. This has also shaped my methodological choices towards participatory and activist methods, discussed further in the section on methodology below.

Attempts to define "feminism" are as fraught and unfruitful as invocations to define other influential and fragmented ideologies such as "liberalism." As a result, many now use the term "feminisms" to indicate the variety of at times contradictory movements under the wing of feminism, including (but certainly not limited to) liberal feminism, intersectional feminism, postcolonial feminism, environmental feminism (Dhamoon, 2013). This move to "feminisms" is useful as it can help avoid what critics have identified as a key failing of White feminism, namely generalising from a White, middle-class experience of womanhood. As Dhamoon (2013) points out, rather than seeing these many feminisms as a problem of unity or coherence, we can understand debates among feminists as a sign of plurality and openness to further reflection, clarification, and inquiry.

In this section, I present what I understand as key elements of feminist scholarship, including (1) using gender as an analytical framework to understand power relations and (2) the move towards intersectionality, positionality, and social standpoint. This understanding necessarily reflects my standpoint (discussed further in the section on Reflexivity) as a white Polish-American woman educated in the United Kingdom. A thesis on feminism written from other standpoints would reflect different interpretations (Dhamoon, 2013).

Gender as an analytical framework

The gender binary is a central concept in many feminist theories. For example, theorists in feminist linguistics posit that, through our use of language, we perceive the world in (gendered) binary, dichotomised, oppositions: hard/soft, aggressive/passive, rational/emotional, technical/social, and public/private (Scott 2012; Tickner 1993). Crucially, these paired concepts are not just binaries but hierarchies, as masculinist norms value the concepts which are gendered masculine more highly. We might praise 'soft' skills or emotional intelligence. However, attributes, personalities, and professions which embody masculine stereotypes are compensated with more power and money in Western culture (Harding 2016).

Following Young (2005), viewing issues through a gender lens means "seeing how a certain logic of gendered meanings and images helps organize the way people interpret events and circumstances, along with the positions and possibilities for action within them" (2005:12). An analytical focus on gender is not necessarily feminist; the key distinction is a feminist perspective, albeit in different ways, puts *politics* – and thereby *power* – at the core of the analysis (Åhäll, 2016; Enloe, 2012).

Oldenziel (1999) charts the relatively recent history of the neologism 'technology', arguing that between 1870 and 1945 in the United States, the term became the exclusive preserve of White, male, educated engineers. Whereas earlier terms such as "the useful arts" had encompassed inventions in agriculture, weaving, teaching or language, the identification between "technology" and "machines" put machines "center stage as the measures of men and markers of modern manliness" (1999:19). Associations between crafts like weaving and femininity as well as "ethnic" or indigenous knowledge served to devalue them, while the notion of technical expertise served to preserve the claim to managerial power of White male engineers. Irani (2018) extends this analysis to demonstrate how "design thinking" articulates a racialised understanding of technical labour and expertise. I argue this process is also evident in the priorities of the cybersecurity establishment.

Gendered ideas shaped what "counts" as a security issue and structures value systems within cybersecurity (this will be expanded further in Chapter 3). Cybersecurity research prioritises *hard* technical problems (such as breaking cryptographic protocols or discovering new vulnerabilities in software) over difficult *soft* social problems (such as preventing coercion of passwords within intimate relationships). In focusing on quantifiable financial risk and military secrets, often within the framework of rational choice theory, cybersecurity also omits emotions and notions of psychological security (L. Stark, 2016). There are gendered patterns in what counts as a cybersecurity issue (financial risk, military secrets), what is excluded (the power

dynamics inherent in corporate monitoring of employee emails), and what counts as a "cool" cybersecurity issue (hacking the hardware, attacks on cryptography). These patterns relate to cybersecurity's origins in engineering but are also gendered in that they prioritise hard over soft, rational over emotional, technical over social, etc. Therefore, feminist theories, which pay close attention to power dynamics as well as feminised concepts like social, emotion, or care, can be a useful corrective to security.

Move towards intersectionality

Many theorists have noted that the primacy of gender as an analytical framework in many feminist theories leads to a reproduction of narrow set of white, middle-class concerns (Collins, 1990; hooks, 1984). Notably, Oyěwùmí (1997) critiques gender and the "woman question" as a Western construct, demonstrating how age and not gender was the primary rationale for organising social worlds in precolonial Yoruba society. Western feminist scholarship then risks recreating the gender binary in its efforts to critique it.

American Black feminists as far back as Sojourner Truth (1851) and the Combahee River Collective (1974-1980) have instead responded to interlocking systems of domination along lines of gender and race. This approach was popularised under the name of "intersectionality" or "intersectional feminism" following Kimberlé Crenshaw's influential (1989) analysis of the ways structural systems of inequality intersect to create unique forms of discrimination that are easily missed when looking at a single category of analysis. A "single axis" focus on cybersecurity as gendered (as opposed to raced, classed, straight, etc.) risks recreating these historical omissions, for example by focusing solely on interpersonal violence and not on violence against individuals by the state (Crenshaw, 1991; Hackworth, 2018a).

The literature on design justice applies this framework to technology design, noting that an intersectional understanding of race, gender, class, and other identities is necessary to support multiply burdened groups of people (Constanza-Chock, 2020). More specifically, Geeng (2022) applies this framework to cybersecurity and threat modelling, explaining that "as a user will face a greater risk of security or privacy violations when an adversary has more power in relation to them", it is crucial for security to understand power across multiple domains such as interpersonal and structural power relations.

Positionality and social standpoint are concepts related to intersectionality which are particularly relevant to academic research. Standpoint epistemology critiques assumptions of objectivity and neutrality in research emphasizes how the knowledge we produce about the world is *socially situated* or shaped by our position within social structures such as race, class,

gender or (dis)ability (Collins, 1990; Haraway, 1988; Harding, 2016)). Moving away from the assumption of objectivity within research has also led many feminist researchers to embrace ideas of research as inherently political. Standpoint theorists often argue for centring the perspective of women or other historically marginalised groups (for example, Black women in the US) as an alternative lens for social science research (Hesse-Biber et al., 2012). Likewise, an awareness of standpoint should invite researchers to reflect on how your own experiences, beliefs, and standpoint in the world shape your research (Gould, 2015). I expand further on my own standpoint in the section on Reflexivity.

Feminist critiques of security

Feminist critiques of security both extend and depart from critical security studies, critiquing security primarily through the analytical lens of gender. Feminist theorists of security have long argued that conventional or mainstream notions of security exclude forms of violence that are deemed "personal" or "private", including gendered violence like domestic or sexual violence (Enloe, 1989; Tickner, 2004b). Feminist theorists traditionally argue that the liberal notion of the home as a private place protected from state power and intervention often shields abuse ranging from casual misogyny through to extreme violence (Suk, 2011). Before the protests of first-wave feminist movements in the 19th century, most legal systems did not prohibit domestic violence, implicitly accepting wife-beating as a valid exercise of a husband's authority over his wife (Clark, 2011).

The meaning of the home as a private space has differing implications among feminist theorists: as Sokoloff and Dupont (Sokoloff & Dupont, 2005) argue, this critique of privacy comes from a position of privilege, as the situation is more complicated for women who are minoritized[1] or have low socio-economic status. As minoritized women and their families are disproportionately targeted by state intervention, the home as a private place shielded from state intervention has a greater resonance. Therefore, calls for the inclusion of these "personal" problems into political framework like the notion of security should be careful of providing justification for unwelcome intrusions into the lives of vulnerable populations. I return to this

[1] The word 'minoritised' "recognises that individuals have been minoritised through social processes of power and domination rather than just existing in distinct statistical minorities" (Law Society, 2022). For example, blue-eyed people are a statistical minority in the population, but are not treated as a racial or ethnic minority as this trait is not racialised. The term also better reflects the fact that ethnic groups that are minorities in the UK are majorities in the global population.

debate in the final section of this chapter, however at this point it is sufficient to note that many feminist theorists argue notions of privacy can reinforce the subsidiary status granted to women's (in)security, so that gendered security threats are 'individualised' and taken out of the public and political domain (Hansen, 2000). This is an example of securitisation and problematisation, i.e., examining how things come to be treated as security problems.

I applied this method of critique to cybersecurity in Slupska (2019) (included in Chapter 3) through examining the security practice of threat modelling-in which security experts systematically identify threats to a device or system. Categorising which threats are included in threat models allows us to understand what kinds of problems security is imagined to address. In Chapter 3, I present a review of smart home security analysis paper which shows that the threat model of intimate partner violence is almost entirely absent in the conventional security analysis literature. I argue that the emerging field of cybersecurity risks recreating the dynamics critiqued by feminist security studies theorists by omitting or dismissing gendered technologically facilitated abuse such as image-based sexual abuse and intimate partner violence (IPV).

This critique also draws on theorists who identify gendered and raced omissions in design practices (Noble, 2018; Criado Perez, 2019). Noble (2018) shows how search algorithms embed racist and sexist bias (or 'misogynoir') so that Google search results for, for example "Black women" or "Asian women" show pornographic images, while searching for "white women" does not lead to overtly sexualised images. Criado Perez (2019) shows how designs in fields as varied as medical research and urban planning are based on data that omits women, leading to fatal flaws like seatbelt designs which do not sufficiently protect womens' bodies. Criado Perez and Noble both link these omissions to the disproportionate power and representation white men hold in technology companies and other sites of design decision-making. Schwartz and Neff (2019) introduce the concept of "gendered affordances" to describe how men and women's differing economic and social standpoints mediate their interactions with "sex-for-rent" ads on Craigslist.

Such critiques can in turn be linked to a longstanding concern in feminist theory with social standpoint (discussed in the previous section). In contrast, conventional threat modelling methodologies which position researchers' imagination of possible threat scenarios as an abstract threat model deploy what Haraway (1988) calls the "god trick of seeing from nowhere", opening the possibility that cultural norms will favour white male standpoints which are obscured by notions of objectivity and abstraction. One way to counter this is to foreground non-expert conceptualisations of security over expert conceptualisations to challenge the belief

"security knowledge held at "the top" is also the "correct" knowledge and that this knowledge will naturally produce effective information security policies and practices."

Standpoint theories which point to the role of researcher or designer identities in reproducing racial or gendered biases should not be reduced to the argument that these omissions will be solved by including more women and minoritized groups in technology design. Such biases occur because of an entrenched culture which privileges a white man as the default user (Criado Perez 2019). As Constanza-Chock (2020) and others have argued, merely including a representative of a marginalised group without changing the broader culture does not address the underlying problem, although it can be an important first step to making these broader changes. Therefore, this thesis does not focus much on the demographics of the cybersecurity and tech industry, although they are heavily skewed[2], and focuses instead on the practices and ideas which contribute to the exclusion of certain threats.

Feminist theories offer not only critiques of security, but also alternative approaches, particularly approaches rooted in notions of safer spaces, eradicating gender-based violence, and care. In response to failures in state and legal responses to address gender-based violence, feminist movements developed both pre-emptive strategies such as consent education and "safer spaces" polices as well as restorative support for survivors with services such as women's shelters and helplines. These action-based strategies at the level of community organising and social activism have also influenced and inspired feminist theorising on the notions of safety and security.

Safer spaces: Addressing gender-based violence

Lewis et al. (2015) note the symbolic significance of violence against women for some feminists, as well as the fact that this significance which has been both claimed and disputed as a ground for feminist politics. The term "gender-based violence", which I use throughout my thesis, is in some ways controversial, because it risks recreating a single-axis analysis which ignores other axes of oppression. I explore these debates further in the next section on technology-enabled coercive control.

---

[2] An obvious example of this diversity problem is the industry's gender imbalance , with only 24% of the global cybersecurity workforce identifying as women (ISC, 2017). Furthermore, representation does not necessarily lead to inclusion: a recent UK study found that while they were not underrepresented in the national cybersecurity industry, Black employees continue to experience significant discrimination in the workplace (NCSC, 2020).

Research about the gendered nature of (both physical and virtual) space, routine abuse and harassment reveals women's negotiations with safety. Feminist debates on privacy and the home as an (un)safe space, have also expanded to consideration of harassment in the workplace or public spaces such as the street. In her study of street harassment, Vera Gray (2018) describes a Catch-22 that women face in developing safety strategies: on the one hand, women are criticised for being too paranoid or narcissistic when they express feelings of unsafety, on the other hand, women are blamed for instances when they are sexually harassed and assaulted, for various behaviours such as drinking or the way they dress. Because of this, there is no "right amount" of panic, "there's only ever too much or not enough. And with no way to know when we're getting it right, we've learnt to just keep quiet" (Vera-Gray, 2018).

Vera Gray draws on the work of Liz Kelly, an influential sociologist on violence against women, who coined the term "safety work" to describe the habitual strategies that women develop in response to their experiences in public (Vera-Gray & Kelly, 2020). Both Vera Gray and Kelly, as well as many other feminist theorists writing in this tradition, focus on the unjust allocation of labour and responsibility in response to problems of sexual violence. They trace how victims of violence are held responsible for the harms that others perpetrate against them. Harris and Woodlock (2019) illustrate a similar dynamic of safety work among survivors of technology-enabled coercive control, in which survivors are expected to keep up with complex privacy and security settings and blamed for not implementing these security practices or using certain platforms or technologies.

A recognition of the various ways women are unsafe both in public and private spaces such as the home has led to long-standing feminist attempts to create "safe spaces" or "safer spaces." Historically, grassroots feminist support services such as women's shelters and rape crisis helplines combined support for those impacted by sexual violence with a political analysis and activism against the role of patriarchy in normalising and upholding sexual violence. One strategy for creating safe spaces which has received significant attention and criticism is "women's only" spaces which exclude men (Lewis et al., 2015). This can apply both to physical spaces (such as women's shelters or feminist conferences) as well as virtual ones: some early online feminist spaces took the "separatist route of excluding males from participation" (Lewis et al., 2015).

Safe spaces can be incredibly questionable both morally and politically as many of these "women's only" spaces exclude trans women, leading to, for example, serious failures to provide services to trans women (even though transgender people are at higher risk of domestic and

sexual violence than cis people[3]) in the gender-based violence sector (Faye, 2021). Furthermore, excluding men does not necessarily equal safety, as studies of, for example, toxicity in online forums such as mumsnet demonstrates (Lewis et al., 2015).

However, experiments with women's only safe spaces have helped to define the meaning of safety for (some) women and in particular, "the meaning and experience of spaces they consider to be 'safe'" (Lewis et al., 2015). Drawing on focus group data with 30 primarily white women in the UK, Lewis et al (2015) "distinguish between safe *from* and safe *to*, demonstrating that once women are safe from harassment, abuse and misogyny, they feel safe to be cognitively, intellectually and emotionally expressive." They argue that due to a significant focus in the literature on safety *from* abuse and misogyny, there is relatively less focus on the important aspect of 'safe to':

> "safe to engage in dialogue, to debate, disagree, challenge, learn; safe to express, to emote; safe to develop one's consciousness, to demonstrate one's creative talent, to fulfil one's potential. This conceptualisation of safety reveals its fundamental importance to ideas of freedom; it is only when we are 'safe from' that we can be free."

Lewis et al (2015) also propose that experiences of public, private and virtual spaces as 'unsafe' combined with being silenced may be conceptualised as constituting threats to 'ontological security' which Dupuis and Thorns (2017) describe as "a sense of confidence and trust in the world, a security of being." This idea of 'ontological security' resonates with scholarship about violence which highlights how coercive control restricts people's capacity to be fully human: for example, Stark (2007:218) highlights how coercive control "by a male partner erode[s] a woman's personhood." For this reason, services such as women's shelters and helplines for survivors have traditionally emphasized safety alongside autonomy and empowerment (Vera-Gray, 2020). These community responses, and the labour required to sustain them, invoke questions of care and (gendered) labour in feminist theories of safety and security, which will be discussed in the next section.

However, before we continue, it is important to note that safety and safe spaces are both subject to critique, just as the concept of security is. Lewis et al note (2015) that, "safety is one aspect of freedom, a necessary requirement for full personhood, but hardly an end in itself." Writing from

[3] This has been found consistently across many national contexts which collect information on gender identity in victimisation studies (Connolly et al., 2021; Williams Institute, n.d.)

an intersectional standpoint, Kishimoto & Mwangi (2009) critique the rhetoric of "safety" in feminist pedagogy, noting how social and technical surveillance can give us a false sense of safety and extending this critique to the notion of a "safe" classroom under a the Western feminist gaze: safety can be used as a pretext to create a "controlled and predictable environment that does not challenge the hegemonic system, thereby ignoring our subjective positionalities." They argue instead for vulnerability in feminist scholarship and pedagogy that calls for "liberation, empowerment, change, and agency."

Srinivasan (2021) helpfully distinguishes between understanding safety as political (i.e., as a good that is differentially distributed across lines of race, gender, class, nationality, and caste) and indulging in an uncontrolled impulse towards safety that can fuel an exclusionary politics, arguing we need to "take safety seriously as a political issue, while refusing a politics of safety." One route to avoiding this hegemonic, controlling politics of safety is to acknowledge that safety is relative: not everyone feels *safe* under the same conditions. For this reason, many spaces (in e.g., nightclubs, conferences, or activism and organising) have adopted the phrase "safer spaces" as opposed to "safe spaces" to indicate that safety is relative and no space is entirely "safe" for everyone (Trans & Women's Action Camp, n.d.). Rather than aiming for perfect safety (or security for that matter), we must aim to make all spaces safer in an ongoing process. This notion of safer spaces is one that I adopt in my thesis.

Care and labour approaches to security

Feminist approaches to security offer a "counter to the selfish pursuit of state or elite security" (Hudson, 2016). When people become the primary referent of security, the emphasis shifts from the security dilemmas of the state to the survival dilemma of people (Hudson, 2016). Intersectional feminism, with its focus on hierarchies of difference, can also shed light on *which* people are the referent object of security. As Hudson (2016) notes:

> "Reflectivist critique and conceptualization of human security by feminists and critical security analysts has done what no other theory of security (and IR) did before: it has made the discipline self-aware and forced – although with obliqueness at times – the discourse outside the confines of mere problem-solving and into the realm of engaging with power."

Hörschelmann et al. (2017) describe social relations as sources of both security and insecurity, or a "key connective tissue through which different dimensions of (in)security are entangled." They describe security practices as including "the emotional and practical labour invested in dealing with the breakdown of social relations." This reflects a broader focus in much feminist

political and ethical theory on the notion of care. In particular, the "ethics of care" is a feminist moral theory which focuses on care as a principle and practice within a wider network of relations between human beings (Held, 2006). Theorists in this tradition often posit that experiences of caring for others, particularly those who are vulnerable, give care-provider privileged access to distinctive and valid forms of moral thought (Held, 2006; Tronto, 1995). Care ethics emphasize the value and necessity of caring labour as well as the values of empathy, sensitivity, trust, and responding to need. Applying feminist care ethics to security, Robinson notes that a feminist "relational ontology reveals the extent to which the continuity of life and a sense of security in people's day-to-day lives are impossible without relations and networks of care and responsibility." Feminist theorists like Hörschelmann et al. (2017) and Robinson (2011) see security as relational (a set of interpersonal practices) rather than individualistic (an individual state). I develop this concept of "networks of care" in Chapter 4 which looks at tech abuse support practices.

Black feminists have also championed the concept of self-care, following Audre Lorde's work on self-care as a radical political act for those burdened within oppressive systems (Lorde, 1988). Akiwowo (2020) extends these ideas to digital privacy, advocating for "digital self-care" (such as muting abusive words on Twitter) and bystander interventions into online harassment. In the words of Saidiya Hartman, "care is the antidote to violence" (Kaba, 2017).

Theorists of care have also introduced critical approaches to care work, focusing for example how unpaid care work furthers gender inequalities (Hester, 2018) and how this disproportionately burdens poor women and women of colour (Hochschild, 2015; Lorde, 1988). Smith and Mackintosh (2007) outlined how traditional care orientated sectors, such as care for older people, are often marginalised because of engrained associations with femininized social roles. Lastly, some theorists have been careful to highlight the "dark sides of care," noting how care can become a cover for control or be disempowering to receivers of care, for example for people with disabilities experiencing medical care (Bondi, 2008). Like safety, care is an ambivalent concept: often treated as an ideal (and perhaps even utopian), yet with a dark side or a history of exclusion in service of this ideal.

Feminist theories, which draw on decades of activism against gender-based violence, offer a variety of potential alternatives to authoritarian, masculinist notions of cybersecurity. The notion of intersectionality highlights how multiple intersecting structures of oppression will put some people at greater risk of security or privacy violations, in contrast to conventional 'neutral' depictions of genderless and raceless technology users. Feminist work on safe(r) spaces highlights both how work towards safety is ongoing and relational (rather than 'solved'

when we reach a state of full security) and how removing threats allows for positive intellectual and emotional expression. Lastly, research on care work and security highlights the forms of labour inherent in dealing with the breakdown of social relations. In the following section, I synthesize these concepts into a conceptual framework and methodology that underpins my thesis.

Methodology: Reconfiguring

Feminist critics of security research and practice call out its omissions, particularly traditional security's failures to address gendered violence. However, as Suchman (n.d.) notes, feminist research shares a commitment to "the critical, but also [to] reconstructive engagement with received conceptions of the human, the technological and the relations between them." Feminist practices and theories, particularly their focus on safer spaces and care, offer potential routes to reform or reconfigure cybersecurity, to make it more caring, and people-centred. Likewise, feminist research methods offer routes to make cybersecurity research more participatory, activist, and reflexive. By combining these approaches, I introduce a critique of and an approach to cybersecurity that is theoretically and empirically novel. In Table 1: Reconfiguring Cybersecurity, I combine these strands into a conceptual framework.

	Current paradigm	**Reconfiguring**
What does cybersecurity protect?	Machine, information, and networks (by extension – their owners)	People embedded in networks of social relations
Who does it protect it from?	Hackers and thieves (external actors)	Other people – particularly those in intimate spheres and positions of power
What damage/harm is important?	Financial cost determined through risk assessments	Suffering (emotional and psychological harm) and reinforcing unjust systems of power
Which methods does cybersecurity use?	Technical analysis, developing security measures (such as access controls)	Participatory and reflexive methods (such as participatory threat modelling)

Table 1: Reconfiguring cybersecurity

As each study uses different methods: threat modelling, participatory action research, and interviews, I will include expanded methods sections in each chapter. However, this section outlines my overall methodology, which is informed by the methodological positions of critical and feminist theories. My critique of much existing security literature highlights how there is too much emphasis on objective understanding, system perspectives and top-down viewpoints (Slupska 2019). My methodological position addresses this through centring the human perspective in a way that is grounded in context and open to elicit the nuance of the everyday experience. This calls for an approach that is qualitative and interpretive (Fujs et al., 2019). Although I have focused my analysis so far on the normative and critical reasons for doing this work, it is also valuable to note that this approach also offers a conceptually interesting perspective on cybersecurity, allowing for nuanced observations about the meanings and implications of security practices that would not be possible with many other methods.

Aradau et al. (2014) note that practicing methods critically means "engaging in a more free and experimental interplay between theory, methods and practice." This recognises that the security practices which critical security scholars research are themselves methods in their own right: for example, as forms of surveillance, data mining, or profiling. Therefore, I use methodological experimentation and innovation as a form of exploring underlying concepts like security and care. As one of the aims of my thesis is to understand whether cybersecurity methods can be adapted to address tech abuse, I adopt conventional cybersecurity methods and reconfigure them using principles and values from feminist theories. In my first two studies, I critique, adopt, and adapt the cybersecurity method of threat modelling using feminist methods. By reflecting on these methods and what kinds of findings they result in, I seek to understand whether and how security practices could be different.

This methodology draws on participatory action research. Action research (AR) is an umbrella term for a variety of approaches in which researchers and participants work together to address a problem and learn from this attempt in cycles of "action" and "reflection" (Gatenby & Humphries, 2000; Kemmis et al., 2014; Kindon et al., 2007a). This stems from the belief that all people affected by an issue should be involved in the processes of research inquiry. Intersectional feminist forms of action research seek to expose the power relations that lurk under the trappings of expertise through methods which empower participants (Gatenby & Humphries, 2000). By combining research and activism, my work rejects the "false dichotomy between scholarship and activism, between thinking and doing" (Collins, 1990).

As a result of the participatory approach of my research, my work is very collaborative. Where possible, I tried to credit people who did different kinds of labour on the projects (including

recruitment, workshop organising, data analysis and not just paper-writing) as co-authors on papers. Throughout the course of my thesis, I co-authored papers, blogs, and reports with more than fifteen different authors. This kind of collaborative work both risks being extractive if done carelessly and can also be in tension with notions of a PhD thesis as the work of a lonely, brilliant individual who "owns" the original ideas they produce. Feminist approaches to epistemology and decolonial critiques of knowledge are sceptical of such individualist notions of knowledge production (Cruz, 2008; Lara Guzmán & Amrute, 2019). Keeping these notions of citation politics in mind, I include a note explaining different co-authors' contributions at the start of each chapter, as well as permission letters showing they are aware of how I have drawn on collaborative work for the thesis. I also intentionally alternate between using "I" for studies and arguments which I developed primarily alone, and "we" for projects and arguments developed with others. However, such a division is inevitably imperfect and superficial: all my thoughts and ideas are heavily influenced by the lineage of theorists and scholars writing before me; collaborators I have worked with or whose work I admire and learned from; and most importantly, participants who shared their thoughts and ideas in my studies.

Lastly, a feminist methodology was also evident in active engagement beyond scholarship throughout my research. This included volunteering at a local listening service for sexual violence survivors (Oxford Sexual Abuse and Rape Crisis Centre) and public engagements which highlighted the problem of technology abuse (such as speaking on the BBC World Service's Digital Planet programme and at the Shameless! Festival of Activism Against Sexual Violence). I also co-authored a commentary highlighting the expertise of advocates and practitioners who support survivors of abuse for the United Nations Institute of Disarmament Research (Slupska et al., 2021). Therefore, alongside my research I engaged with survivors and communicated the importance of this subject to audiences beyond academia such as advocates, security practitioners, and the public. Lastly, I practiced reflexivity throughout the research process, outlined in the following section.

Reflexivity and positionality

In my second year of research, I started a reflexivity journal and planned to write in it weekly. However, I found this difficult and unproductive, and ended up only sporadically noting down reflections. Instead, inspired by Strohmayer's (2020) "Sewing through the pandemic" project, and researcher practices of reflexivity through narrative practice and textile-making (Arias López et al., 2021; Bishop & Shepherd, 2011), I started an embroidery project which materially represents the way various life experiences, forms of positionality, and both academic and non-academic texts influenced by research formulation and methodology choices (see Figure 3).

This stitching journal helped me reflect on my work, resulting in the reflections on positionality below.

Figure 3: Embroidered reflexivity journal; intertwined lines resemble influence of various personal and academic experiences on my work

Starting a cybersecurity course within a computer science department made me at times uncomfortably aware of aspects of my identity—namely, being a woman and a social scientist—which were positioned as 'outsider' to cybersecurity research and invalidated in various subtle and unsubtle ways. Frustration with these forms of invalidation contributed a lot to the feminist framing of the thesis, as feminist theory helped me articulate the benefits of my perspective as a woman and a social scientist to the field of cybersecurity. It made me reflect on my own gendered experiences of harm and feeling unsafe (as well as supporting friends through similar experiences), which I believe give me a valuable and underrepresented perspective on security and shaped the focus on safety throughout this thesis. These experiences of harm were also part of my motivation for volunteering with the Oxford Sexual Abuse and Rape Crisis Centre, which created a mixed insider/outsider identity when interviewing advocates who support survivors of sexual and domestic abuse (see Chapter 4).

The various ways in which I am an 'insider' to and benefit from structural privilege (such as being white, middle class, cis and educated at university whose prestige and power is linked to colonialism) as well as the ways this shapes my work were less immediately obvious to me and

required more reflection (which, like other aspects of reflexivity, is ongoing and incomplete). Fo example, my father and older brother are programmers, both working in cybersecurity for parts of their careers. This gave me a level of access and familiarity with the subject even before I received any training. Furthermore, my research recreates the Eurocentricity and Anglo-Americanism of my educational background, which is a serious limitation given how overrepresented these 'minority world' countries are in academic research (discussed further in the Limitations section below and in the Conclusion). Furthermore, as I do not have formal training in feminist theories (outside of some courses on feminist International Relations and feminist critiques of technology), my understanding of different feminisms is self-taught and patchy. As I started to read more of Black and intersectional feminisms, I reflected on how my position as a white woman at Oxford shapes my work. For example, in focusing on the "private is political", I initially paid insufficient attention to harms perpetrated by the state (a common result of single axis "gender analysis") (Sokoloff & Dupont, 2005). I found hooks' (1986) and Dabiri's (2021) work on solidarity particularly helpful for thinking through these issues. hooks (1986) outlines how white women's identification as "victims" of misogyny can preclude them from exploring the impact of their own race and class privilege and doing the "dirty work" necessary to build political awareness and solidarity. Drawing on hooks' work, Dabiri (2021) calls on white people to avoid denial and guilt spirals and focus on supporting and joining coalitions to fight systemic racism which do not centre white people or white peoples' experience.

Similarly, in the first stages of the Reconfigure research project (described in Chapter 3), we attempted to make feminist cybersecurity spaces that were welcoming to women and non-binary people, but by recruiting among our own social networks and locally in Oxford, we ended up with groups which were predominantly white, highly educated, and progressive, etc. In later stages of the project, we collaborated with Voice of Domestic Workers, a group representing migrant domestic workers in ways that more actively incorporated the framework of intersectionality and ethic of solidarity . This raised new questions of outsider perspectives and mitigating power dynamics in research (discussed further in Chapter 4).

Limitations

Although the limitations of each individual method will be discussed in each chapter, my overall methodology shares some consistent limitations which could be expanded in future work.

First, my work lacks a clear geographical scope, although as I mentioned before, it broadly recreates the Anglo-American focus that is already highly prevalent in research on cybersecurity as well as technology abuse. Although Study 2 did involve several participants

situated in the Global North or in 'in-between' areas like post-Soviet states, my Anglo-American education and location is evident in both methods (workshops held locally in Oxford or London, overrepresentation of American practitioners interviewed etc.) and in the general formulation of my ideas. There is a risk here that I implicitly generalise my findings from an Anglo-American context as if this were universal. I have mitigated this by emphasizing perspectives from outside of the US and the UK both in my literature review and in my findings.

Second, while focusing on feminist and intersectional approaches to security and technology, I have not included theories on how technology design reinforces other axes of oppression, such as disability or queer theory. Understanding how these structures shape cybersecurity would be a fascinating and very important area for future research.

Third, due to the short timescale of this research, I did not complete full cycles of action and reflection which are preferable for participatory action research. This means for those studies which were interventions on participants lives (such as the cybersecurity workshops), I usually did not follow up to try to understand the impact of these interventions.

Lastly, my methods—which are qualitative and interpretivist—are not meant to be generalisable or objective (Fujs et al., 2019). However, in this rejection of notions of objectivity and positivism, I have also avoided quantitative methods in a way that verges on methodological sectarianism. A true openness to methodological experimentation would also include a greater willingness to engage in methodological pluralism.

Avoiding co-option

As cybersecurity is a particularly masculinised field at the intersection of technology and security, feminist approaches are necessary correctives. However, feminist politics and scholarship themselves should not be put on a pedestal, as various feminisms can be exclusionary or subject to co-option. Notions like safer spaces or care should not be treated as panacea, as intersectional and disability justice critiques of these concepts demonstrate. In proposing positive visions of security as care, we must also be mindful of critiques of care, such as how unpaid care work furthers gender inequalities (Hester, 2018); how this disproportionately burdens poor women and women of colour (Hochschild, 2015; Lorde, 1988); and how care can become a cover for control, for example for people with disabilities experiencing medical care (Bondi, 2008).

These critiques of care echo critiques of White feminism more broadly: in particular, how White feminism tends to universalise from a White, upper-class women's perspective (Davis, 1981; Hooks, 1984; Jonsson, 2016) or justify further interventions into over-policed communities

through a focus on penal solutions for intimate partner violence, discussed further in the literature on 'carceral feminism' (Bernstein, 2012; Srinivasan, 2022). Focusing solely on violence at an intimate scale within the public/private binary can obscure and omit other structural harms and state violence. This is a particular risk for any project that seeks to develop a feminist security, as highlighting security problems experienced by women provides can be co-opted to provide justification for further expansions of the carceral state. Theorists of feminist security have noted the risks of "securitising feminism" (Srinivasan, 2022; True, 2012) in a way that reinforces oppressive logics of security. Notably, since the time I began this thesis, harms like intimate image abuse have been criminalised in the UK and many other countries.

In the field of cybersecurity, co-option could look like setting up invasive surveillance systems in the name of defending against GBV. For example, in the early stages of my research, when I decided I wanted to focus on intimate partner violence, a computer science professor encouraged me to try quantitative methods and specifically suggested using machine learning to develop an image recognition algorithm that could spot visual signs of abuse such as bruises from women's social media posts. This suggestion, which seemed both unethical and ineffective, nonetheless illustrated a tendency to use surveillance and automated categorisation in response to social problems.

Is it possible for security to be caring or even emancipatory practice, or will it inevitably introduce a carceral logic identified by critical scholars of technology? Some theorists see potential for a reformed, feminist or human-centred security, while others see it as inherently oppressive, and argue instead for values like safety, empowerment, or liberation. My work contributes to this debate by testing out the viability of a feminist (cyber)security by incorporating feminist notions like care, intersectionality, or including the standpoints of conventionally excluded groups. Both critical and feminist critiques of security usually focus on the omissions and hierarchical tendencies of military or corporate security. There is relatively little work exploring security practices in defence of those with relatively less power in society, such as those affected by intimate partner violence and coercive control. For this reason, digital security practices in response to technology-enabled coercive control form the overarching case study of my thesis. By studying security in this context, I aim to shed light on this underlying question of whether and how (cyber)security can account for power relations.

To summarise, some feminist theorists do see a possibility for a feminist security in response to problems such a gender-based violence. However, it is a mistake to take it for granted that security *should* be feminist, because being feminist is not automatically good. The utopian ideals of feminism can be and have been riddled with exclusion and oppression and co-opted by

broader forces like capitalism and the carceral state. This raises questions which those who (like me) identify as feminist scholars and activists must grapple with: why is it that some feminisms have been co-opted so easily? Is it possible to learn from past mistakes and avoid feminism being co-opted in similar ways in our (post-)digital context?

This leads me to an underlying question in my work, i.e., *should* we reconfigure cybersecurity to address tech-enabled abuse. In her influential critique of white feminists, the poet and theorist Audre Lorde (1984) reminds us that "the master's tools will never dismantle the master's house." If the concepts, practices, and tools of (cyber)security were forged to defend the powers at the top of any given hierarchy—the sovereign head of state, the CEO in the boardroom, the head of the household—can they truly be reconfigured to defend vulnerable and marginalised people? Or will the notion of feminist cybersecurity only serve to "pink-wash" a more palatable version of the same drive to secure technology (and therefore the owners of the technology) over people? In other words, is reconfiguring cybersecurity a type of "reformist reform", which lessens some of the negative effects of a system to keep the overarching system of oppression in place?

I return to these questions in the conclusion of my thesis. However, for the time being, I argue that reconfiguring cybersecurity is useful, as the field has a significant amount of resources, expertise, and power over design decisions. Using the language of cybersecurity allows us to draw on cybersecurity methods and speak to a field that has the power to change technology design. However, this does not eliminate the difficult question of whether a framework developed primarily for the protection of digital property belonging to militaries and corporations can be reconfigured to protect marginalised people. This thesis addresses this question through empirically exploring potential sites of alternative approaches to security practice, as a case study grounded in an empirical phenomenon can provide a way to make these considerations more concrete. In the following section, I introduce and define the phenomenon of tech abuse, and explain why it is a useful case to examine what a feminist security may look like in practice.

Tech abuse as a central case study

Understanding responses to the phenomenon of technology-enabled coercive control or "tech abuse" forms the central case study of my thesis. I am interested in whether responses to the problem of tech abuse resemble a feminist form of cybersecurity, due to the history of feminist activism on gender-based violence and resulting theorising on safety and security. If

cybersecurity methods are deployed to address the newest, tech-enabled manifestation of misogyny, does that make cybersecurity feminist?

In this section, I first define the phenomenon of tech abuse, and then review existing literature on tech abuse. Most existing research on tech abuse (both in social science and more technical approaches such as security and privacy research or research on human-computer interaction) have either (1) built an understanding the dynamics of tech abuse or (2) developed solutions that aim to reduce this kind of violence. Both these kinds of work can jump to conclusions about what researchers, developers, or designers should do to tackle this issue. My research likewise attempts to develop solutions, but I also contribute to a third strand which seeks instead to empirically study existing responses to tech abuse within the violence support sector.

Defining and understanding tech abuse

Coercive control is a pattern of behaviour that is designed to assert influence and control over an individual's life using threats of harm, dependence, isolation, intimidation, and/or physical forms of violence, often resulting in a survivor losing a sense of their self-worth, bodily integrity, and safety (Cuomo & Dolci, 2019; Stark & Hester, 2018). Coercive control is increasingly used instead of "domestic violence" to encompass situations in which partners are not cohabitating, as well as to highlight that not all abuse includes physical violence. Technology-enabled coercive control refers to forms of coercive control which incorporate (usually digital) technology; in other words, the deliberate use of technologies or systems to scare, harass, coerce, or stalk someone. Throughout this thesis, I use "tech abuse" as a shorthand for technology-enabled coercive control to simplify the language.

Drawing on past work defining the tech abuse threat model (Freed et al., 2018a; Henry & Flynn, 2019; Levy, 2019; Slupska & Tanczer, 201.; Tseng et al., 2020), there are five primary forms of tech abuse perpetrators use:

- Ownership-based access: Being the Owner of a device or account allows a perpetrator to prohibit victims'/survivors' usage or track their location and actions.
- Account/device compromise Guessing or coercing credentials which enables a perpetrator to install spyware, monitor the victim/survivor, steal their data, or lock them out of their account.
- Harassment: Contacting victims/survivors or their friends, family, employers etc. without their consent, often including deception, defamation, or impersonation.

- Malicious exposure: Posting or threatening to post private information or non-consensual pornography (i.e., image-based sexual abuse).
- Gaslighting: Making a victim/survivor feel as if they are losing their sanity and/or control over their home, for example by remotely changing temperature using an IoT device or deleting past messages and denying they were sent.

Previous literature reviews have shown a consistent, and slow stream of qualitative research documenting IPV survivors' experiences and advocates' reports of technology-enabled abuse (Brown et al., 2018; Woodlock, 2017). Perpetrators of tech abuse usually do not use highly technically sophisticated techniques. Instead, since perpetrators are often living with their victims or have intimate relationships with them, they often gain access to victim's accounts through physical access to victims' devices, knowledge of victims' passwords, or their ability to guess or coerce these passwords. As a result, many conventional security measures based on an authentication model, such as passwords and security questions, are not effective in preventing tech abuse. Freed et al. (2018) describe the prototypical tech abuse perpetrator as a "UI-bound adversary" who uses the existing interfaces of apps and platforms for abuse, rather than finding exploits in code. When these forms of access are not enough, perpetrators also have easy access to stalkerware programs which enable location-monitoring and other forms of stalking (Chatterjee et al., 2018). Such applications are sometimes available on app stores and may even be in-built into our everyday devices, such as 'Find My Friends' or similar location-sharing applications. Other researchers have examined the role of platforms or emerging technology like IoT in mediating abuse (Lopez-Neira et al., 2019; Parkin et al., 2019; Tanczer et al., 2021a).

Like all forms of abuse, tech abuse is both gendered and intersectional. Women, non-binary, and trans people experience domestic and sexual violence at higher rates than cis men. These forms of abuse are also underpinned by societal structures of oppression such as racism, class privilege, ableism, heterosexism (Gray, 2012; Hackworth, 2018b; Sokoloff & Dupont, 2005). People experience oppression at the intersections of these different aspects of their identity, forming multiple kinds of complex experiences (Crenshaw, 1991). For example, while women experience domestic and sexual violence at disproportionate rates, poor women, women of colour, and immigrant women are also further marginalised when law enforcement do not take these experiences seriously or even penalise survivors of abuse(Crenshaw, 1991). Most of the existing research also focuses primarily on Global North, English-speaking countries like the US, UK, and Australia, and therefore fails to account for regional and cultural specificities (Sambasivan et al., 2019). For example, in India, devices are often shared widely in the household and having personal laptops or smartphones is rarer. Therefore, models which speak of "device compromise" reflect a kind of Eurocentric bias which assumes individual device

ownership; peoples' expectations and negotiations of privacy are shaped by differing regional and cultural contexts.

These forms of abuse are also sometimes referred to as cyberviolence, digital gender-based violence or digital harassment, which each term implying a slightly different set of phenomena. These terms also include harassment by strangers on online platforms such as Twitter (J. Fox & Tang, 2017; Hackworth, 2018b; L. M. Jones & Mitchell, 2016; Mahar et al., 2018). In contrast, I focus primarily on ways in which technology is co-opted for coercive control in intimate relationships, such as family or dating violence. However, I also include any violence from which co-opts or weaponizes technology for coercion and control within the label of "technology-enabled coercive control."

These forms of abuse can and do happen outside of familial or romantic relationships: for example, technology-enabled stalking or intimate image abuse are harms which are often perpetrated by clients against sex workers (Bowen et al., 2021). Likewise, harms such as "sextortion"-in which the threat of releasing intimate images is used to coerce someone into acts such as sending more intimate images, are sometimes perpetrated by partners or family members, but can also be perpetrated by strangers who specifically target victims on online forums or dating apps (Wittes, 2016). Coercive and controlling relationships can also happen between employers and employees, particularly where large power balances exist such as in the case of migrant domestic workers who work in the intimate spaces of the home. Although these various cases encompass many different dynamics and contexts, they share the elements of coercion, control, and weaponised intimacy which are key elements of this study.

Responses, solutions, and solutionism

As a result of socio-economic, legal, and familial reasons, many victim-survivors must live with tech abuse for many years. In many cases, ending technology-mediated abuse is not as simple as securing devices or changing passwords. In this section, I outline existing work that has responded to this kind of abuse.

Following empirical research to understand practices of perpetrators and needs of survivors, researchers turned their attention towards finding solutions. I differentiate between three areas of solution-oriented work: (1) recommendations for survivors; (2) technical recommendations; and (3) the development of services, particularly through community-based action research projects. I argue that, while it is important for research to explore and recommend solutions,

this is not the only way to approach this problem and can in fact miss an important step: i.e., closely studying existing security practices.

Responses to tech abuse, particularly from law enforcement, often include recommendations for survivors to keep themselves safe. These risk imposing an additional burden of safety work on survivors who are already psychologically, financially, and emotionally burdened by abuse, or creating new forms of victim-blaming in which survivors are accused of having inflicted harm upon themselves by choosing to use certain devices and/or platforms (Harris & Woodlock, 2019). Sim (n.d.) traces how victim-blaming logics can also be embedded in "anti-rape technologies", by prompting users to collect certain kinds of information to prove the veracity of their claims instead of believing them.

Technical solutions have included design recommendations (Hussain, 2021; Levy & Schneier, 2020; Nuttall et al., 2019) and methods such as threat modelling (Slupska & Tanczer, 2019) co-design with survivors (Leitão, 2019) and usability analysis (Parkin et al., 2019c) for the design and development of safer systems. Chayn, an organisation which uses crowdsourcing to aid survivors of gender-based violence, has developed design principles for "trauma-informed" design, which works to create interfaces and services that acknowledge how experiences of trauma affect individuals and groups (Hussain, 2021). Sim and Zevenbergen (2017) develop design ethics for gender-based violence and safety technologies, such as being cautious of defaults that connect the user to law enforcement, co-designing with survivors, and being vigilant and cautious of harms that can come from research.

There are also examples that have put into practice some of these recommendations, such as Arief et al.'s (2014) platform for survivors, the Tech vs Abuse project (TechvsAbuse, 2019), or Unmochon, a tool for publicly sharing evidence of harassment (Sultana et al., 2021). An app named "myPlan" in the US draws on violence research to help survivors access information to assess their risk, gain access to services, and consider their options (N. Glass et al., 2015; N. E. Glass et al., 2021). These approaches are valuable, as they highlight the role of technology design in mediating and enabling abuse and offer technology companies ways to address and mitigate technology abuse in design. It is important for companies to understand they have a responsibility to address these problems on their products and platforms. However, problems of abuse cannot be "designed out" or "solved" by UX changes (Blythe et al., 2016).

Other solutions have included recommendations of support systems, such as calls for "networks of empathy" from technologists, police officers, educators, and employers (Kadri, 2020) and legal and policy recommendations (Citron, 2019). Alongside academic research, "grey literature" (such as non-academic reports and guidance documents) from women's support

services (Woman's Aid, 2018), sex worker organisers (Hacking//Hustling, n.d.) , or organisations working on online gender based violence (Glitch, 2020) has also centred the testimonies of survivors, provided timely empirical research about experiences of harm and violence, as well as opportunities for the development of services to support perpetrators in changing their behaviours (Bellini et al., 2020).

Although empirically studying tech abuse advocates' security and safety practices has not been the focus of much existing research, some valuable exceptions include studies of ecosystems of support for tech abuse survivors (Freed et al., 2017), safety planning practices in domestic violence shelters (Murray et al., 2015) and the information security needs of human trafficking services (Chen et al., 2019). These studies emphasize the difficulties and importance of balancing information security and psychological safety for survivors as well as technology as a "double-edged sword" which both enables survivors and exposes them to risks. Lastly, not all survivors can access conventional victim support services. For example, Sambasivan et al. (2019) emphasize many survivors' preference for seeking support from friends and family, and Zou et al. (2021) investigate the role of customer support in an anti-virus company in aiding survivors.

Two projects have combined developing solutions with empirically studying the support sector by setting up clinics where technologists support survivors in securing their devices. The Clinic to End Tech Abuse in New York, USA, has described existing ecosystems of support for tech abuse survivors (Havron et al., 2019), produced resources and checklists for securing survivors accounts and devices (CETA, n.d.), and explored the challenges of providing services to survivors during the covid-19 pandemic (Tseng et al., 2021).

The Technology-Enabled Coercive Control Initiative is a community-based participatory action research project in Seattle, USA, in which researchers collaborate with advocates to better understand the problem of technology-enabled coercive control (Cuomo & Dolci, 2019). Their research has both helped define the problem of tech abuse, highlighting how tech abuse can be debilitating and cause feelings of hopelessness in survivors, and also understand gaps and failures in support systems. They emphasize that the process of seeking relief and accountability through civil and criminal legal systems is often ineffectual and can even be retraumatising.

Both these initiatives focus on "building bridges" between the victim-support sector and law enforcement, researchers, and technology companies to more effectively provide relief (Cuomo & Dolci, 2019). These projects have highlighted broader legal and policy changes which must

happen to address the rise of technology-enabled abuse: for example, although tech abuse clinics have made significant contributions in local contexts, significant funding and investment would be needed to make these services accessible more broadly (Freed et al., 2019). Similarly, a recent study of the intimate partner violence support sector in the UK highlights the shortcomings of existing risk assessment and recording practices as well as the urgent need for greater funding to develop the sector's capacities (Tanczer et al., 2021b).

Lastly, Kazansky (2021), in her study of resistance to data-driven surveillance among civil society organisations, provides an empirical study of threat modelling practices in the third sector (i.e., outside of state or corporate practices). She points out the ways that the language of threat modelling can reproduce a security mindset that focuses on the worst-case scenario, which can be intimidating for groups facing serious targeting by powerful actors such as the state. She notes that some organisations prefer neutral terms like "context analysis" instead of "risk assessment" or "threat modelling" which might be stressful or intimidating.

To summarise, many researchers have started developing solutions at individual, technical, and societal levels. However, these papers generally do not provide a comprehensive look at what security practices look like in the sector. Instead, they often point towards spaces that require improvement, in what can be called a deficit model for research: looking for what needs fixing, but not looking at innovation that is happening among practitioners and what we can learn from it. Furthermore, most of these papers-particularly those coming from computer science, privacy and security research-do not include any power analysis of the broader social structures that produce insecurity. Many of them do not even mention gender as a factor in intimate violence. Instead, there is a tendency to see the newest, tech-enabled manifestation of intimate partner violence as a new engineering problem, rather than an old and complex social issue.

This raises broader questions about the nature of responses and solutions to deep-rooted social problems when they re-appear in new, "digital" or "technology-enabled" forms. Critics of tech "solutionism" such as Morozov (2013) have identified a tendency for tech developers to attempt to exploit the power of technologies to solve social problems in an engineering mindset that can be short-sighted and self-interested. Morozov argues for "responses" to complex social problems over "solutions." It is valuable to note that civil society and third sector organisations are themselves not impervious to tech solutionism (Bellini et al., 2020). However, studying responses to tech abuse in the support sector offers a valuable case study for understanding responses outside of the short-term fixes of tech solutionism. Furthermore, this offers a

valuable case study for understanding feminist (cyber)security practices in a vastly different environment to the military and corporate contexts in which security practices are usually located.

Conclusion

A feminist critique of cybersecurity notes how it is masculinist, particularly how it protects technology and wealth at the expense of at-risk and marginalised people, such as survivors of intimate partner violence. This reflects and expands broader critiques of security as an oppressive construct, which leads some to argue for rejecting a security mindset altogether. Although I find this argument compelling, in this thesis I take a somewhat different route, exploring how cybersecurity may be reconfigured to be more people-centred, drawing on feminist notions of care and safer spaces. Feminist approaches are a useful starting point for correcting these omissions in cybersecurity, as feminism is historically concerned with the problems of gender-based violence and coercive control. For this reason, studying responses to the phenomenon of tech abuse is a particularly informative site to explore alternative, feminist forms of security. The following chapter starts this process by expanding the cybersecurity method of threat modelling to include the context of intimate partner violence.

However, this objective also raises the broader question of whether security being feminist is inherently desirable. Critiques of (for example) neoliberal, carceral or White feminisms have shown how the feminist movement has been repeatedly co-opted by broader social structures like capitalism or the carceral state towards undesirable or even oppressive ends. Security *can* be feminist, but this is not a panacea. Ultimately, we must remain reflexive and critical of power relations and treat security and safety not as end goals in themselves, but preconditions for liberation and empowerment.

Chapter 3: Threat modelling intimate partner violence[4]

Chapter summary

Feminist theorists of security have long argued that gendered binaries of public/private work to diminish the importance given to domestic or private insecurities, so that these security problems are 'individualised' and taken out of the public and political domain. This chapter argues that the emerging field of cybersecurity risks recreating these dynamics by omitting or dismissing technology-facilitated coercive control. Through the case study of the August smart lock, I show how gendered assumptions and omissions can translate into security design and affordances. I then present a review of forty smart home security analysis papers to show the threat model of tech abuse is almost entirely absent in this literature. I develop a threat modelling method for smart home systems in the context of coercive control and intimate partner violence. Lastly, I explore limitations in this approach and how this opens space for further problematisation of threat modelling.

Introduction

"And so you're back
From outer space
I just walked in to find you here with that sad look upon your face
I should have changed that stupid lock, I should have made you leave your key If I'd known for just one second
you'd be back to bother me"
- I Will Survive (Gloria Gaynor)

The act of changing a lock to prevent someone from accessing your home is a crucial act for personal security amid a relationship breakdown. This means the design of this lock is political

[4] Author statement: this chapter was written based on two papers titled "Safe at Home: Towards a Feminist Critique of Cybersecurity" in the St Antony's International Review and "Threat modelling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things" with Leonie Tanczer. As sole author for the first paper, and first author on the second, I was responsible for overall research design and led on paper writing. Dr Leonie Tanczer collaborated on every section of the threat modelling chapter. For this chapter, I combined sections of both papers, removing the background and literature review (which is broadly repetitive of Chapter 1), and expanded on our methods in greater detail than paper limits allow.

in a feminist sense. If this lock is connected to the internet, its access configurations dependent not on a locksmith, but on Wi-Fi connections, servers, access control settings, and user-interface design. Gendered assumptions in the design and development of these different systems and configurations therefore has crucial security implications. Security analysis papers—a genre of information security research in which researchers assess the security design and potential avenues for compromise in a system—offers a way to understand these assumptions and omissions.

This chapter combines two threads of work: first, a critical review of existing security analysis research on smart home devices shows limitations in existing approaches to threat modelling (Slupska, 2019). Second, a co-authored chapter with Dr. Leonie Tanczer adopts and adapts the existing method of threat modelling for the context of coercive control (Slupska & Tanczer, 2021.) I offer two important contributions: I show how by using gender as a category of analysis, critical theory can pinpoint oversights in security analysis. This offers a detailed answer to RQ1, showing how assumptions in problem formulation mean security practices fail to account for tech-facilitated coercive control. Second, I offer a pragmatic contribution and a remedy to this oversight by developing a detailed threat modelling method that designers and developers can adopt and adapt to anticipate abuse. This offers the beginning of an answer to RQ2 – although as I discuss in the conclusion, this method on its own is incomplete. By reflecting critically on omissions in a mainstream security method, and by showing how this method can productively be applied to the problem of technology abuse, I offer pragmatic routes for improving cybersecurity.

Gendered gaps in smart home security analysis

Cybersecurity research often starts by "threat modelling"—a security design method in which experts anticipate potential threats to a computer system. The literature on threat modelling is complex and full of jargon. It is a field populated by acronyms such as DREAD[5] and STRIDE[6] and characterized by debates about the distinction of *threat* and *risk* (Xiong & Lagerström, 2019). Although there are many different formats for threat modelling (e.g., asset-based,

[5] i.e. Damage, Reproducibility, Exploitability, Affected User, Discoverability, (see https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model))

[6] i.e. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) (see https://en.wikipedia.org/wiki/STRIDE_(security))

system-based, and attacker-based), this process usually involves mapping out the relevant components of technical system, listing possible threats and vulnerabilities, and identifying mitigations which can minimise or eliminate the risk of a breach (for a detailed review, see Shostack 2014).

Although often presented as abstract and impartial, this process usually relies on security experts' own experiences and assumptions about everyday users (Benenson et al., 2015a). As Wyatt (2008) notes, to understand the role of 'users' in technology development, we must "distinguish between 'real' users in the 'real' world and the images of those users and their relationships held by designers, engineers, and other sorts of system builders." One example of this is the assumption that threat actors are external to the home.

As I outlined in Chapter 2, a key element of many feminist theories is using the gender binary as an analytical framework. The binary of "public" (i.e., political, masculine) vs "private" (i.e., personal, feminine) operates to exclude many issues central to women's lives from the realm of "politics" (Scott 2012; Tickner 1993). This explains how problems of domestic and sexual violence were historically (and to some extent presently) excluded from public conversations. As Enloe (2019) notes, family homes have been designed and redesigned according to gendered notions of housework and feminine respectability, reflecting underlying power and labour dynamics in the homes. In particular, the liberal notion of the home as a private place protected from state power and intervention often shields abuse ranging from casual misogyny through to extreme violence (Suk, 2011). Unfortunately, the emerging field of cybersecurity has not incorporated these insights and therefore risks omitting many forms of technological abuse.

To illustrate this problem, I review two papers which assess the security architecture of a smart lock and show that their threat modelling does not sufficiently account for technology-enabled coercive control. I show how applying gender as a framework for security analysis can point to omissions such as assuming the "owner" of the house is not a threat. Although later chapters move beyond this "single-axis" focus on gender, this case study offers a useful introduction to socially situated analysis in security. Last, to demonstrate that this is not an isolated oversight, I present the results from a comprehensive review of smart home security analysis papers.

The August Smart lock system

In this chapter, I use the case study of the August smart lock, an early entry to the smart home market. I choose the case study of a prototypical smart lock system because it has relatively simple functionality (i.e., opening and closing a door) and plays a key role in home security (i.e., allowing and preventing access).

The August smart lock is a round knob which attaches to the inside of a standard deadbolt lock. The smart lock can be physically turned from the inside to open or lock the door. It also allows a user to lock or unlock the door electronically using a mobile app on their smartphone. To do this, the smart lock connects to a user's smartphone using Bluetooth. The smartphone app communicates with the smart lock's company's web servers via Wi-Fi.

The company's web servers describe both hardware and software components which store, centralize and manage the files a user requests when engaging with a company's website or app. The smart lock's setup means that the device itself is not directly connected to the Internet. Instead, the smart lock communicates with the smartphone app via Bluetooth. Therefore, for this threat model, the smart lock *system* consists of a) the smart lock; b) the smartphone app; and c) the company's web servers which support the app (see Figure 2).

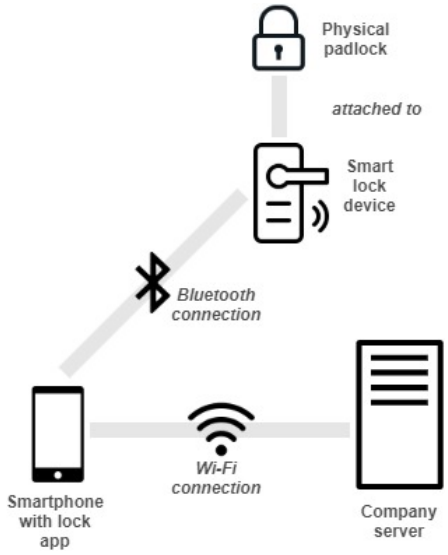

Figure 2: Overview of the smart lock system.

The smart lock has two "modes" for opening doors: either the user manually opens the smartphone app and presses a large button to open the door, or the door is set so that the lock opens the moment the phone is within Bluetooth range. The smart lock device also records which users lock or unlock the door, storing the data on the smartphone app and in the web servers.

Users identify themselves by logging into the smartphone app with their phone number or email address and a corresponding password. There are two different user account types: "Owner" and "Guest." The first and original user is *by default* an Owner. However, the device

allows multiple Owners and Guests. The Owner is effectively the administrator of the system. They have more privileges than Guests. For example, an Owner can view the lock's activity log (i.e., past accesses), invite new users to be Owners or Guests and configure when and for how long Guest users can lock/unlock the door (Ur et al., 2013).

Capability	Owner	Guest
Lock/unlock door	Yes	Yes
View activity log	Yes	No
Invite new users to be Owner or Guest	Yes	No
Remove Owner or Guest access	Yes	No

Table 2: Account capabilities (adapted from: Ye et al., 2017b).

Users cannot access another user's account without having access to a fellow user's credentials. However, the main Owner can remove other users—both Owners and Guests—without having to access (i.e., login) their accounts.

Smart lock security analysis papers

Fuller et al. (2017) and Ye et al. (2017) both conducted a security analysis of the August Smart Lock. Both papers prioritise a model in which a thief attempts to gain illicit access to the house as well as a scenario in which an adversary with temporary guest-level access such as an 'Airbnb tenant or a household worker' change*s* their settings to gain access at a different time. In these cases, the owner is automatically assumed to be the defender, rather than a potential threat. This is reminiscent of the issues identified in Chapter 1, where a similar assumption was made at the cost of domestic workers.

Fuller et al does consider the following scenario:

1. Alice gives Bob Owner-level access.
2. Alice gets out of Bluetooth range of the lock.
3. Bob maliciously puts his phone in airplane mode, preventing it from communicating with the August servers, but leaving Bluetooth enabled.
4. Alice revokes Bob's access.

In this case, because Alice cannot communicate with the lock (as she is out of Bluetooth range) or Bob's phone (as he has disabled Internet connectivity), the lock cannot receive the message

that Bob no longer has access. This means Bob, who is no longer a legitimate user of the lock, can enter the home at will until Alice is within Bluetooth range. Fuller et al point out that there also appears to be a bug in the lock's logging code, so that the log files will not report Bob's access during this period.

However, Fuller et al. (2017) are surprisingly dismissive of this security vulnerability, saying it is alarming in theory, but unlikely to be a problem in practice, given that:

> "Owners, by definition, can revoke each other's access. In fact, if Bob were truly malicious, he could have revoked Alice's access after he was granted OWNER status. For this reason, the original owner should not give OWNER status to anyone she does not trust immensely."

Both prongs of this argument are highly questionable. The fact that a malicious Owner can immediately and effortlessly revoke a legitimate Owner's access to the house should be considered a potential threat. Similarly, in the context of a relationship ending, it is unfortunately the case that immensely trusted parties can suddenly become adversaries with the intention to cause harm. Saying that Alice should not give Owner status to someone she does not trust also places responsibility on her rather than the manufacturer to prevent her own abuse. This question of responsibility is one I will return to in the final section of this chapter.

Of course, in any scenario in which cohabitants lose trust in each other, the question of which inhabitant is a legitimate owner is much more morally and legally fraught than in the examples of a thief or an errant Airbnb guest. However, security system policies cannot simply ignore these issues, given the serious harm that can result from domestic abuse and stalking.

Broader review of smart home security analysis

The following section presents the results of a review of the wider smart home security analysis academic literature. To gather a comprehensive data set, I conducted a search in the SCOPUS academic database and collected 40 smart home security analysis papers.[7] I coded each paper according to what artefact it analysed and which threat models it considered (see Appendix I). The papers varied in specificity, with some analysing a specific product (like the Samsung SmartThings platform) while others considered 'Internet of Things' (IoT) or 'smart home'

[7] A search for ('security analysis' AND smart AND home) yielded 82 documents. To focus on influential papers, I removed all documents which had no citations, leaving 49 documents. A further nine documents were removed because they did not relate to smart home technology (seven) or because they did not conduct a security analysis (two).

devices more broadly (see Table 1). 16 papers explicitly mentioned potential threat actors (either in the introduction or as a formal part of the threat model), resulting in 29 threat actors identified in the sample (see Table 2).

Remote network-based attacker	7
External adversary	6
Internal adversary	5
Burglar/thief	2
Privileged insider	2
Arsonist	1
Bad manufacturer	1
Home intruder	1
Malicious user	1
Physically present attacker	1
Revoked attacker	1
Suppliers and drivers	1
Total	29

Table 2: Threat Actors Considered in Sample Papers

The representations of threat actors in Table 2 and threats in Table 3 below do not seek to categorise threat models, but rather to show how they were represented in the sample papers. For example, some of the more specific threat actors mentioned, such as 'Arsonist' or 'Home intruder' could be grouped as external adversaries; however, I have included them to retain the level of specificity in the papers.

Intimate partner violence or an abusive partner or family member was not mentioned explicitly in any of these papers. Arguably, some of the listed threat actors – such as 'Internal adversary', 'Privileged insider', or 'Malicious user' – could include the IPV threat model. But closer inspection shows this is not the case, as all seven papers which consider 'Internal adversaries' or 'Privileged insiders' discuss 'insiders' as employees of the organisation which sells or

operates the device. Furthermore, the paper which discusses the 'malicious user' threat actor conceives the user as a threat to the *manufacturer* (rather than other members of the household) as the user might 'learn the secrets of the manufacturer, … sell secrets to third parties, or even attack similar systems.'[i]

The threats considered also reinforce the assumption of a remote, network-based attacker or an external threat such as a thief. The most common attacks – Eavesdropping, Replay, DoS, and Man-in-the-Middle attacks all refer to network-based subversion of security infrastructure. While a domestic abuser could of course theoretically launch any of these attacks, existing research shows that such abusers often use attacks which require only basic computing skills and are unlikely to rely on sophisticated methods. In contrast, the threats associated with the IPV threat model – such as privacy breaches, or illicit attempts to enter the home – appear very rarely in the literature. Fuller et al.'s security analysis of the August Smart Lock, despite its somewhat dismissive treatment of this threat model, is therefore actually the only paper in this sample which considers a home intrusion by a revoked owner of the device.

Threat modelling tech abuse [8]

In this section, I develop a method to threat model smart home devices in the context of intimate partner violence and coercive control more broadly, drawing on earlier work with Dr Leonie Tanczer. As I discussed in Chapter 2, there are various approaches to threat modelling, ranging from: a) asset-based threat modelling; and b) system-based threat modelling; to c) attacker-based threat modelling (see Shostack, 2014). These approaches can also be combined to generate an illustration of the system that is potentially being attacked, assumptions about the profiles of potential attackers, including their goals, methods, and motives; and a catalogue of likely threats that may arise. In this case, we use the case study of a smart lock based on the August smart lock (an early entry to the smart home market), however this method can be applied to other smart home devices more broadly. Likewise, we limit the attacker 'type' to one scenario: technology-enabled coercive control. Therefore, we combine elements of system- and attacker-based threat modelling.

Following Shostack's (2014, p. xxvii) suggested system-based approach, threat modelling involves four steps, each answering a deceptively simple question:

---

[8] The authors are indebted to Adam Shostack and Eireann Leverett, who kindly provided feedback on earlier drafts of this book chapter. Parts of the insights discussed in this publication stem from findings derived from UCL's "Gender and IoT" research project.

a) What are you [i.e., the tech vendor] building?
b) What can go wrong with it once it's built?
c) What should you do about those things that can go wrong?
d) Did you do a decent job?

Although system-based approaches such as this one are implicitly aimed at tech developers and vendors, we believe it is valuable for anyone studying tech abuse—whether from the perspective of social or computer science—to be comfortable with the conceptual framework of threat modelling. The latter allows researchers to reflect, understand, document and react to the possible shortcomings of digital devices and services (Sabbagh & Kowalski, 2015; Torr, 2005). By becoming fluent in the language of threat modelling, IPV scholars and practitioners can more effectively critique problematic technology designs. In the upcoming section, we walk readers through the building blocks of this framework to showcase the benefit of its adoption in the tech abuse space.

We draw on the four questions outlined by Shostack (2014), and use the upcoming passages to:

a) Model the relevant features prevalent in common smart lock systems (what are you building?)
b) Show how specific features may be abused (what can go wrong?)
c) Suggest possible mitigation strategies (what should you do about those things that can go wrong?)
d) Discuss limitations of the threat model we developed (did you do a good job?)

In the current threat modelling analysis, we are foregrounding the device rather than its user or its interplay with the broader system of interconnected products (i.e., how a smart speaker interacts with the smart lock). We acknowledge that this viewpoint has limitations; as the common security saying goes "all models are wrong; some models are useful." For one, an IoT system cannot be viewed as a purely "technical" problem. In most cases, social and technical aspects are tightly interwoven, requiring both social and technical countermeasures (Sabbagh & Kowalski, 2015). As I discuss in the conclusion of this chapter, these kinds of changes will not "solve" the problem of tech abuse. However, as technology design can exacerbate the problem, preventative design is an important part of the response. For another, investigating a single device over an assembled system allows for vulnerabilities to pass through undetected (J. R. C. Nurse et al., 2017). While we accept that one must account for the entire IoT "ecosystem" (Aufner, 2020; Omotosho et al., 2019; Seeam et al., 2019), a broader investigation is beyond the scope of this chapter.

System: What are you building?

The threat modelling process begins with collecting necessary information about the relevant components of a device, software program or system (Torr, 2005). This decomposition gives stakeholders an overview of all the different segments, data points and interactions to effectively identify, understand and model its make-up (Xiong & Lagerström, 2019). Developers begin by creating simple diagrams and tables to provide an overview of the system being threat modelled. These diagrams can clarify different interdependencies and features of systems, which are particularly important for smart, Internet-connected devices (Steven, 2010). For tech designers and vendors, these visual representations form a useful way to abstract all system properties and diagnose what an application does (Coles & Tarandach, 2020).

As I have already described the August smart lock system in Part 1 of this Chapter, I will not repeat it here.

Threats: What can go wrong with it once it's built?

After the exposure of the "anatomy" of a system, tech vendors use the generated diagrams to look at what could go wrong. As there is an unlimited number of things which could fail, this second step has the potential to be the most overwhelming. The evaluation of interconnected systems such as IoT technologies creates an additional level of intricacy than the analysis of individual devices and application alone. However, in both cases, tech designers should assess opportunities for abuse across the whole infrastructure (Coles & Tarandach, 2020).

Some approaches start by profiling probable attackers, including their resources, motivations and capacity (Atzeni et al., 2011; Little & Rogova, 2006). The identification of an attacker's intentions can assist in the forecasting of an attack's sophistication level, which is particularly useful when examining IPV cases. The threat identification process involves a certain reliance on assumptions as to the nature of a likely perpetrator. These assumptions are often limited and stereotypical (Atzeni et al., 2011), which is – considering the lack of diversity among cybersecurity practitioners, as well as the lack of data on tech abuse – problematic (Lopez-Neira et al., 2019; Poster, 2018).

Having a diverse team is vital for threat modelling. Institutional and personal life experience shape perceptions of threats. Thus, technologists who specialize in Windows systems will often skew their threat model towards Windows-specific concerns, while web developers will be primarily focused on web-based attacks. Equally, our own biases as authors of this chapter will have influenced the threat actors and attack scenarios we are examining. To mitigate such

shortcomings, we want to reiterate that active collaboration with affected groups and communities such as the domestic abuse sector must be sought.

When looking at an attacker's profile, both their opportunities for exploitation and/or their attack motives can be significantly influenced by environmental conditions. For instance, a perpetrator with a background in software development may be far more likely to consider exploiting smart home devices. Nonetheless, an attacker's capacity must be contrasted, considering their potential motivation. Depending on both aspects, one must expect changes to the: a) intensity; b) sophistication; and c) probability of a tech abuse attack taking place; as well as d) a perpetrator's ability to distort/eliminate forensic evidence (UcedaVelez & Morana, 2015).

Based on the current evidence-base, tech abuse perpetrators are often highly motivated or even obsessed with the desire to monitor, coerce, intimidate, or otherwise harm a victim/survivor. They can, but do not have to, be physically present (Ho et al., 2016). Abusers are also rarely strangers. They often have or had romantic relations with victims/survivors. Nonetheless, tech abuse can also be perpetrated by family members, colleagues, roommates or acquaintances (Levy, 2015). IPV perpetrators often have intimate knowledge of the victim/survivor, including awareness of their daily habits, history and login details, or access to personal data like sexually explicit or embarrassing photos and messages.

In addition to this profiling exercise, it is helpful to account for known attack patterns (UcedaVelez & Morana, 2015). Drawing on Freed et al. (2017) and Leitão (2019), we propose a model of five common tech abuse threats:

Name	Description
Ownership-based access	Being the Owner of a device or account allows a perpetrator to prohibit victims'/survivors' usage or track their location and actions;
Account/device compromise	Guessing or coercing credentials which enables a perpetrator to install spyware, monitor the victim/survivor, steal their data or lock them out of their account;
Harmful messages	Contacting victims/survivors or their friends, family, employers etc. without their consent;
Exposure of information	Posting or threatening to post private information or non-consensual pornography (i.e., image-based sexual abuse);

Gaslighting	Using a device's functionality (e.g., remote changing of temperature) to make a victim/survivor feel as if they are losing their sanity and/or control over their home.

Table 1: Tech abuse threat model.

These threats can be connected to the specific features of the device to identify which forms of tech abuse are possible/likely (as we do in the following section). The second step ends with documenting as well as rating all diagnosed threats (Meier et al., 2003).

There are countless possible threats that could apply to a smart lock, some of which have already been explored by cybersecurity researchers (Fernandes et al., 2016; Pavelić et al., 2018; Ye et al., 2017a). However, our model of IPV threats outlined earlier helps to focus on specific "attack vectors" (i.e., methods by which an adversary may gain access to the lock), followed by eight "threats", (i.e., specific forms of abuse which can occur after a lock has been compromised).

a) Ownership-based access: Perpetrator has an Owner account and revokes and/or monitors a victim's/survivor's access.
b) Smartphone compromise: Perpetrator illegitimately accesses the victim's/survivor's phone while within reach of the smart lock, which offers them digital access to the app, as well as physical access to the property.
c) Account compromise: Perpetrator coerces or guesses victim's/survivor's smartphone app *or* smart lock account details, which allows the perpetrator to log into the victim/survivor's account on the perpetrator's own smartphone or laptop.
d) Smart lock compromise: Perpetrator physically damages the smart lock making it unusable or causes a power outage which in certain circumstances may restrict residents from entering the house/locking the door.
e) System compromise: Perpetrator can use default functions of the smart lock as some poorly designed IoT devices allow anyone on the same Wi-Fi home network to control an Internet-connected product.

We acknowledge that it is possible to deploy more technically sophisticated attack scenarios (Ye et al., 2017b). However, the attack vectors discussed here showcase the range of relatively simple attack vectors that are available to the "UI-bound adversary." These attack vectors enable some of the following forms of abuse, or "threats":

a) Restricting access: Perpetrator removes the victim/survivor's account and/or changes their password, which can restrict the victim/survivor's access to their account, as well as the shared home. This can be particularly damaging in the context of cohabitation where physical residency can impact decisions on ownership in court settlements.
b) Gaining access: Perpetrator maliciously gains access to the property even after the victim/survivor attempted to lock them out. This can result in physical or psychological harm to the victim/survivor and/or their family.
c) Monitoring: Perpetrator monitors the victim/survivors and/or other residents through the account access log. This can facilitate stalking or coercive control by giving the perpetrator the exact times that a victim/survivors and/or other residents enter and exit their home (Ur et al., 2013).

d) Exposing information: Perpetrator uses the information received from an account compromise to coerce or expose the victim/survivor. This can result in personal information leakage (e.g., address) which threatens the user's privacy.
e) Impersonating users: Perpetrator compromised the account of another resident and uses these credentials to access the property unnoticed. This engenders the physical safety of the victim/survivor and/or fellow residents.
f) Gaslighting: Perpetrator unlocks the door just before the victim/survivor arrives home, making it seem like the device is malfunctioning or the door was never locked in the first place. This may result in victim/survivors doubting the functionality and security guarantee of their smart lock.
g) Contacting victim/survivor: Perpetrator tries to enter the property with an unauthorised smartphone, which leads the victim/survivor receiving a notification (Khalid & Majeed, 2016). This can cause distress and anxiety for the victim/survivor who now has an awareness of the perpetrator's access attempt.
h) Distracting and deceiving: Perpetrator argues that they had previously physical access to a device such as a victim's/survivor's smartphone which could give them the impression of an attacker having more access than they do. Akin to gaslighting, this can cause a victim/survivor to feel uncertain about their level of security and safety.

The power dynamics inherent to IPV cases add further complications to the scenarios expressed here. Tech abuse stemming from ownership-based access seems particularly likely, as the Owner of a smart home device has an inbuilt advantage in monitoring and controlling other users (i.e., members of the household). Geeng and Roesner (2019) show the "outsized role of the person who installs devices in terms of selecting, controlling, and fixing them." Research has also demonstrated the gendered aspects of "digital housekeeping", namely that men are more likely to set up and maintain smart home technologies (Kennedy et al., 2015; Leitão, 2019; Strengers et al., 2019). Therefore, account ownership may reinforce power inequalities in the household related to gender, technical ability or finances (as these dictate who purchases devices).

Furthermore, even if a victim/survivor is the authorized Owner of the smart lock, the removal of the perpetrator's account – whether they have had previously held legitimate Guest access or have been detected to have received access to the account illegitimately – can expose the victim/survivor to further risks of violence and abuse. The act of withdrawing a perpetrator's admission can escalate the abuse situation and could cause perpetrators to react (e.g., confront or harm the victim/survivor). For this reason, mitigations to tech abuse – which are discussed hereafter – must be highly context-specific with designers minimizing the risk of abuse independently of user's ownership status.

Response: What should you do about those things that can go wrong?

The third question involves the examination of countermeasures to tackle each threat. Conventionally, responses are (a) to reduce/mitigate threats through the implementation of

safeguards and changes to eliminate vulnerabilities or block threats; (b) to assign/transfer threats by placing the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing; or (c) to accept the threat by evaluating if the cost of the countermeasure outweighs the possible cost of loss due to the threat. While the full elimination of threats is generally possible, it would require almost always the removal of features which industry actors may be opposed to (Shostack, 2014).

Mitigations are consequently specific to a device's design goals and conventionally limited by a vendor's resources, interests and capacity. Therefore, this step also involves prioritizing different threats to identify which mitigations are most urgent. In the private sector, such assessments are often quantified and based on financial losses. Tech vendors have so far struggled—and often failed—to incorporate more intangible social, emotional, or psychological harms, including damage to reputation or mental health implications. The industry's viewpoint on the importance of economic ramifications disproportionally disregards the broader implications technical innovations may have on different groups of society, which we aspire to alleviate in this chapter. However, many of these limitations are inherent in the approach to "system-based" or "device-based" threat modelling, which inherently contains a tech solutionist framing.

Various research teams have already emphasized possible tech abuse responses industry actors, policymakers and support services can deploy (Havron et al., 2019; Leitão, 2018; Lopez-Neira et al., 2019; Parkin et al., 2019; L. Tanczer et al., 2018). However, it is important to stress that technical mitigation strategies will not exhaustively "solve" the problem. As in other attack scenarios, security is never perfect or absolute and technical solutions need to accompany robust social and legal support for victims/survivors. By the very nature of tech abuse – which includes the notion of the *authenticated adversary* – compromise and security breaches are *always* likely. Thus, one cannot prevent an IPV attacker by simply establishing *conventional* technical barriers (e.g., implementing a firewall, setting up password protections) as there are no trusted "safe zones" victims/survivors can rely on (Weinert et al., 2019).

As seen through our proposed mitigation strategies, many design choices may equally benefit victims/survivors as much as perpetrators. Thus, we are fully aware that an adversary may co-opt our proposed strategies to gain access or control victims/survivors further. However, some design decisions can enable harm more easily than others. Consequently, rather than looking to eliminate sources of vulnerability, we believe it is more useful for industry actors to think in terms of beneficial design patterns. The latter are likely to *enable* usability for people

experiencing abuse and *hinder* usability for those perpetrating abuse. Tech abuse stemming from the following compromise forms may consequently be mitigated by:

Ownership-based compromise:

a) Restricting ownership: As preventing ownership-based access is impossible, security designs should give Owners less exhaustive authority over the smart lock system. This may include a security protocol which allows the company to remove an Owner in exceptional circumstances, such as when requested by a domestic abuse court order.
b) Equalizing account holder rights: Moving away from models where only one user is an account Owner or doing away with an Owner/Guest user distinction.
c) Consent changes: Shared IoT devices such as smart locks may require all associated users to approve fundamental changes to the settings which prevent Owners from overpowering others.
d) Customer-facing staff guidance: Akin to the "Assisting Customers Experiencing Domestic and Family Violence Industry Guideline" (Communications Alliance Ltd, 2018), customer-facing staff guidance on how tech vendors can support tech abuse victims/survivors may be developed to assist users in the instance of disputes around who is a legitimate account holder (L. M. Tanczer, 2019).

Smartphone compromise:

e) Report theft feature: A "report theft" feature could be activated from the victim's/survivor's web account to minimize the access a perpetrator may have over a device such as their smartphone.
f) Automatic log outs: Users could be automatically logged out of their accounts, requiring them to re-authenticate themselves on timed patterns when using their smartphone to lock/unlock a smart lock. This may prevent unauthorized usage by others should the phone ever get lost.

Account compromise:

g) Register of login details: Regular notifications of login locations (i.e., where) and associated timestamps (i.e., when) may be accessible to victim's/survivor's through their account settings (Parkin et al., 2019). Crucially, these should be sufficiently vague so as not to put a victim/survivor in danger should a perpetrator access this information.
h) New login prompts: Accounts may trigger a notification when a login on a new IoT devices is attempted.
i) Changing of passwords prompts: A new login should be required across all devices if a user changes their password, to ensure that other users do not stay logged in after, for example, a breakup.
j) Reinstate account ownership: The ability to reinstate access to previously compromised accounts may be mitigated through time-stamped company back-ups which can allow victims/survivors to regain control over their data (e.g., after a court order).
k) Multi-factor authentication: Different authentication methods should become part of the IoT design feature and may ensure that accounts are less prone to, for example, password coercion (Leitão, 2018).
l) Transparency around privileges: Users on lower authorization levels (i.e., Guest accounts) should receive continued reminders of the extent of information they, in comparison to other account holders, such as "Owners", receive. This may alert

victims/survivors to the fewer privileges they hold compared to their partner and remind them that a perpetrator could have access to their activity log.

m) Access trails: IoT devices could notify other users ever time another account holder checks critical settings such as access logs. This may prevent obsessive or routine checking of another user's behaviour as the monitoring individual would be informed about this action.

Smart lock compromise:

n) Factory reset: IoT devices should enable a simple mechanism to reset the product to its original state, enabling victims/survivors to restrict access after a compromise or breakup occurred. In the context of IoT, this mechanism needs to be both simple to activate (e.g., through a button) and potentially difficult to pursue from outside the home Wi-Fi network. Once initiated, the device should also send a final "good-bye" message to all users, which would alert them to an illicit factory reset.
o) Logs: Victims/survivors may need to provide proof that a breach of, for instance, a protection order has occurred. Access logs such as who has accessed, locked, unlocked the door should, therefore, be unchangeable for any account holder.
p) Disable functionalities: Users should be able to decide if they would like to disable certain functionalities such as the remote closing/opening of a smart lock.

System compromise:

i) Connection reminders: Regular prompts reminding users which IoT devices are connected and which accounts are associated with them may flag to victims/survivors if a perpetrator is still linked to their appliances (Parkin et al., 2019).
j) Opt-out: IoT devices should allow users to opt out from distinct data collection measures which are not required for the essential functionality of a connected product. This aligns with data minimization principles.
k) Actionable advice: Up-to-date guidance on what steps a user should take when they suspect their home network has been compromised must be available to victims/survivors and communicated in a simple and understandable format (Parkin et al., 2019). A dedicated button that says "I am a victim/survivor of domestic violence" or "I am worried about threats from a former partner or housemate" could automate access to this guidance.

Across this section, we have shown that threat modelling does not need to be complex to be useful. Indeed, our suggested set of mitigations emphasize how such an approach can be both practical and feasible. More research is undoubtedly needed to define, test, and improve our privacy and security propositions—not only to evaluate their effectiveness, but to identify further technical response means. Nonetheless, based on the current state of knowledge, we are confident that the above-mentioned design choices could mitigate harms stemming from IPV compromises and further benefit the "average" IoT users whose level of privacy and security is enhanced by these measures.

Validation: Did you do a decent job of analysis?

The final question involves a critical reflection on the efficacy of the generated threat model. To support this evaluation process, different validation methods can be deployed (Xiong & Lagerström, 2019). What unifies these methods is their attempt to check the model's completeness and accuracy. The scrutiny guarantees that the final model matches the system that is built, addresses all the right and relevant threats and covers all the decisions that have been made (Shostack, 2014). By this stage, every possible attack scenario should have been considered and accounted for and a planned countermeasure laid out.

A common practice to support this step is the reliance on "test cases" or "case studies" (Shostack, 2014; Xiong & Lagerström, 2019). Another form of explanation and validation includes collecting data on device usage "in the wild." Moreover, data on reported breaches can be helpful, especially if contrasted with initial threat models to understand whether a threat was inadequately addressed or missed entirely. Together with a frequent reiteration of the threat modelling exercise, new and unanticipated threats can be accounted for, and timely and effective mitigations strategies implemented.

We are conscious of the limitations that underpin our "IPV Threat Model" and the restrictions that derive from our reliance on a single, hypothetic test case (i.e., smart lock). Instead of checking our model for its completeness and accuracy, we consequently hope to have showcased how design features in the context of IoT systems can shape and embed power dynamics and stimulated a discussion which may lead to changes in industry practices.

Our current threat model was built on several qualitative tech abuse studies which compiled the experiences of victims/survivors and support organization (Dragiewicz et al., 2018; Freed et al., 2017, 2018a; Harris & Woodlock, 2019; Leitão, 2018; Lopez-Neira et al., 2019; Parkin et al., 2019; Slupska, 2019). Testimonies of victims/survivors are a critical way to validate a model. This can be done by checking that the model and analysis produced a set of threats that includes what is in the literature, as well as other sources of victim/survivor testimony.

However, it would make for a more robust model, if future threats and attack vectors could be derived from detailed qualitative and statistical data gathered by statutory and voluntary support organizations, academia, and industry stakeholders (for example, through compiling user complaints). The reliance on multiple data sources will also mitigate potential biases that derive from various forms of victims/survivors under- or non-reporting of abuse (Fernández-Fontelo et al., 2019). As scholars such as Tanczer et al. (2018) have highlighted, once more detailed accounts of the frequency, extent, regional specificities and nature of tech abuse cases have been collated, more targeted mitigations strategies can be developed. Thus, the tech sector

will have to become comfortable and able to amend and redesign systems after their deployment. In the long run, this will benefit not only IPV victims/survivors, but also the conventional users who gain from the security and privacy improvements that can be designed and implemented.

Conclusion

This chapter identifies a systematic omission in conventional cybersecurity analysis: threats to the smart home are understood to come from 'outsiders' such as hackers, thieves, or corporate sabotage. People within the home, or conventional users, are either ignored or not considered as threats worthy of taking seriously in the models used for security analysis. Using a feminist analysis which understands the personal as political, I argue this is a serious mistake: due to power dynamics such as gender, race, age, or disability, actors in the home may have very different powers over each other and can and do pose serious risks to other inhabitants' security. This is complicated even further by the case of domestic workers in the home, which I examine more closely in Chapter 4. The second part of the chapter addresses this gap by developing conventional threat modelling methods to consider the context of coercive control and think systematically about how design features may facilitate or mitigate the risk of abuse. I return to this question of 'abusability' in Chapter 6. This is an important contribution as intimate partner violence and coercive control cause enormous harms in society; as these harms are increasingly facilitated by technology, it is critical that the field of technology design and security have models and frameworks for mitigating these harms.

However, at this point it is crucial to note three key limitations in the approach taken in the second part of this chapter, which I advance in further chapters. Firstly, this "system-based" form of threat modelling—which starts with a specific device like a lock—implicitly limits the potential scope of solutions to the design of the device. It is unlikely to include broader responses such as a customer support helpline that aids people trying to identify or mitigate abuse. Additional limitations and constraints are often imposed through corporate frameworks such as identifying less "resource intensive" solutions. Mitigations such as hiring moderators or setting up customer support helplines—not to mention implementing a restorative justice process—will naturally be more "resource intensive" than a user interface design change. However, this kind of framing does not allow for broader conceptions of structural justice: i.e., if companies have accumulated large amounts of resources through creating products and platforms which facilitate harm, the fact that some actions are "resource-intensive" should not be used to dismiss them. Yet many forms of threat modelling, which weigh the costs of risks and mitigations using cost-benefit analysis, can reify this kind of thinking.

Secondly, as discussed above, it is often impossible to distinguish abusive from non-abusive uses of a device without considering context and intentionality. Limiting threat-modelling to security analysis of a system can lead one to the exasperated conclusion that every mitigation can also be abused in some way, so there is nothing one can do. This again is because system-based threat modelling limits the locus of intervention to the device design, rather than broader support, education or conflict resolutions systems which might operate at the level of the individual, relationships, or a community as a whole.

Lastly, although we drew on the existing body of research with survivors of abuse, this type of threat modelling still positions the security researchers as the authority on deciding "what could go wrong." This makes it likely that significant omissions will continue to occur, as security researchers come with their own assumptions and limitations. The next chapter further problematizes the assumptions underpinning threat modelling, asking not only "who do we consider as a threat?" but also "who gets to define threats in the first place?"

Chapter 4: Participatory Threat Modelling[9]

Chapter summary

The cybersecurity method of threat modelling involves systematically mapping assets, threats, and mitigations to a technical system such as a server or a smart lock. This chapter introduces a new method that reconfigures threat modelling to put the needs of people, rather than those of a technical system, at the centre of the threat model. This new method of participatory threat modelling (PTM) draws on long-standing traditions of feminist participatory and activist research methods, allowing security research to incorporate power imbalances and centre marginalised peoples' experiences. Developing and improving this method through a series of 12 workshops with various community groups forms one of the major contributions of my thesis. By asking participants to define their own threats, my research collaborators and I developed more robust threat models which included structural factors which create insecurity. Drawing on the framework of intersectionality, we also map how different forms of threat can reinforce each other, such as the way insecure immigration status makes migrant domestic workers more vulnerable to online scams and harassment. These methodological, empirical, and theoretical contributions provide a model for more grounded and engaged security research, and a call for security researchers to join community support networks in coalition and solidarity.

Introduction

What threats count in cybersecurity? As a field, cybersecurity can seem obscure and daunting to outsiders, a domain for hackers, cyber-warriors, and technical experts. Yet, everyone is exposed to potentially vulnerable technology and made more vulnerable by technology. By drawing on

---

[9] Author statement: this chapter was written based on two papers titled "Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity" with Scarlet Dawson Duckworth, Linda Ma, and Gina Neff and "'They Look at Vulnerability and Use That to Abuse You': Participatory Threat Modelling with Migrant Domestic Workers" with Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. As first author for both papers, I was responsible for overall research design, participant selection and recruitment for the workshop, interviewing participants, initial data analysis and coding, and approximately half of both papers. The remaining authors helped with workshop organising, grant applications, data analysis and paper writing. For this chapter, I combined sections of both papers, removing the background and literature review (which is broadly repetitive of Chapter 1), and expanded on our methods in greater detail than conference paper limits allow.

these experiences of vulnerability, rather than abstracting away from them, cybersecurity can become more relevant to everyday concerns.

In this chapter, I introduce the method of participatory threat modelling (PTM), which I identified and developed over the course of this study in collaboration with my co-authors. PTM combines the cybersecurity practice of threat modelling with long-standing traditions of feminist participatory and activist research methods. To do so, I describe a series of workshops in which "non-experts" (such as migrant domestic workers, activists, and members of the public) defined their own threats. Rather than focusing on a specific device, threat actor, or problem (which reflect researcher priorities), PTM is an open-ended method which follows participants' own experiences and definitions. In this way, PTM combines the structure of threat modelling with a values-based focus on empowerment and care that characterises feminist participatory research. Although many others have employed threat modelling techniques with activists, human rights organisations, and marginalised groups (Kazansky, 2021), to my knowledge this is the first effort to systematise it as a research method. By involving participants in analysis and reflection, I also enhance researcher-led sense-making with participants' input. PTM extends my response to RQ2 (how to use participatory and feminist methods to reconfigure cybersecurity).

PTM illustrates the importance of privacy and security to everyday lives, while simultaneously reconfiguring security to be more grounded in people's concerns. This is a model for more grounded and engaged security research: resulting in a call to join community support networks in coalition and solidarity. In this chapter, I first outline the conceptual framing of the study, then detail our method and process, before presenting our results and discussion. Developing and improving this method through a series of 12 workshops with various community groups forms one of the major contributions of my thesis. Throughout this process, the project also changed significantly, from one-off workshops with the public, to a year-long collaboration with Voice of Domestic Workers, a support group ran by and for migrant domestic workers. My reflections on the iterative, complex and at times messy nature of the project are a critical part of this methodology.

By asking participants to define their own threats, my research collaborators and I developed more robust threat models which included structural factors which create insecurity. These threat models form the empirical contribution on this chapter. These innovations in methodology and empirical findings also lead to a theoretical contribution. Drawing on the framework of intersectionality, we map how different forms of threat can reinforce each other, such as the way insecure immigration status makes migrant domestic workers more vulnerable

to online scams and harassment. Therefore, this method offers a clear foundation for reconfiguring cybersecurity to account for abuse and power relations. Instead of suggesting new technical solutions in isolation from practitioners on the ground, digital security researchers can build with existing sources of safety by partnering with community organisations to develop their information security capacity and dismantle oppressive structures. Participatory threat modelling offers researchers a method to implement this.

Problematising threat modelling

As I discussed in the previous chapter, threat models also reflect researchers' positionality: consider the example of the "evil maid threat model" that I discussed at the outset of the thesis. Imagining a domestic worker as a potential threat, rather than as a security subject, implies a privileged position defending those already in power. By positioning the researcher's imagination of possible threat scenarios as an abstract threat model, such methods deploy what feminists have critiqued as the "god trick of seeing from nowhere" (Haraway, 1988). In contrast, feminist standpoint theories advocate for the use of socially situated experiences as an alternative lens for social science knowledge (Haraway, 1988; Harding, 2001; Hesse-Biber et al., 2012). Activist (or "action research") and participatory methods offer a methodology to implement this theoretical approach to knowledge, forming the methodological component of reconfiguring cybersecurity. By seeing research participants as "experts of their own experiences", methods which draw on standpoint theory consciously reject the idea that, e.g., security experts have superior or even more relevant understandings of what threats count in cybersecurity.

Activist or action research (AR) methods reject notions of research as impartial or neutral, seeing all research as a form of intervention. By choosing instead to join existing communities and/or activist groups, researchers can learn about a problem through taking action to address it. Action research involves cycles of action and reflection in which researchers and participants work together to address a problem and learn from this attempt in cycles of "action" and "reflection" (Hayes, 2011; Kemmis et al., 2014; Kindon et al., 2007b). This stems from the belief that all people affected by an issue should be involved in the processes of research inquiry (Kemmis et al., 2014). For example, Pain et al (Pain et al., 2010) describe a participatory research project which involved farmers, environmentalists, engineers, and academics in a project on about environmental concerns in a local river. Projects with community partners result in more socially relevant, collaborative, and engaged research.

There is evidence that these kinds of projects help bring women and other underrepresented groups into computing (Hayes, 2011). Yet action research in cybersecurity and other technical

fields is exceptionally rare (Fujs et al., 2019). AR projects are relatively more common in the adjacent field of Human-Computer Interaction (HCI). However, HCI AR projects usually consist of the "deployment of novel technologies" (Hayes, 2011). This reproduces a narrow understanding of what solutions to social problems may be, and precludes legal, economic, political, or cultural change. This speaks to the importance of the *stage* at which participatory approaches are used: i.e., research design (which included problem framing), data collection, data analysis, etc. As Smith et al. (2010) note, the term "participatory action research" is sometimes incorrectly applied to projects where community partners are only brought in at a late stage.

Starting the collaboration earlier allows for valuable input on the scope and subject of the research, which can shed light on researcher preconceptions. Community engagement in problem framing counters this tendency, for example by uncovering how framing algorithmic harms around "bias" suggests that more accurate data is the solution, at the risk of missing deeper questions about whether surveillance technologies should be used at all (Katell et al., 2020).

Other research traditions focus on how to make technology design processes more just and equitable. Value sensitive design (VSD) examines how both pre-existing and emergent biases manifest in computer systems and proposes methods for designers to consider the values of various stakeholders (Friedman et al., 2009; Friedman & Kahn, 2002). Calls for "feminist HCI" often centre values such as agency, fulfilment, identity, equity, empowerment, and social justice (Bardzell, 2010). Feminist and anti-racist critiques move beyond an unconscious bias framing to show how intersecting structures, such as patriarchy, white-supremacy, ableism, and heterosexism are "hard-coded" into technology, often reproducing existing forms of oppression under the guise of technical neutrality (Benjamin, 2019c; Noble, 2018b; Wajcman, 2009). The design justice movement seeks to "retool" design methods by centring the voices of those who are directly impacted by the outcomes of the design process (Costanza-Chock, 2018).

All these initiatives build on a growing recognition that harms associated with technology impact different groups of people differently. Recent security research has focused on the needs of groups facing specific forms of marginalisation, such as undocumented migrants (Guberek et al., 2018), refugees (Simko et al., 2018), sex workers (McDonald et al., 2020; Strohmayer et al., 2019), queer people (Geeng et al., 2022), intimate partner violence survivors (Freed et al., 2019; Leitão, 2019), and activists (Albrecht et al., 2021). This has led to calls for a recognition for "differential vulnerabilities" (Pierce et al., 2018) and a third wave of "inclusive privacy and security", as "people from different under-served groups may have profoundly different needs

and challenges for security and privacy" (Wang, 2018). Marginalised people experience a disproportionate amount of state and other forms of surveillance; for example, those who rely on public benefits must share "personal information [...] far more routinely than wealthier citizens" (Green & Gilman, 2020; Madden et al., 2017).

Participatory security design avoids the assumption that the security of the individual will follow from the security of a technical system and includes the perspective of actors who may ordinarily be marginalized (Heath et al., 2018). Thus, participatory methods incorporate 'situated' knowledge and practices (Haraway, 1988) to ground information security studies. Researchers have used participatory security design methods in studies of privacy mechanisms for smart homes (Yao et al., 2019) and security and privacy threats with survivors of intimate partner abuse (Leitão, 2019). In such research, users define or reframe digital security threats, showing how "differential vulnerabilities" can be socially contingent based on factors such as gender, race, or age (S. Fox et al., 2018). For example, when asked to define "cyber security" children focus more often on predatory or bullying behaviour, while adults focus on financial crimes and technical protection (S. L. Jones et al., 2019). However, participatory security research which directly involves marginalised groups in problem framing and security design is still exceptionally rare.

Moving away from a focus on technology design, security researchers can support marginalised groups through directly providing technical support and advice. For example, tech abuse clinics (Cuomo & Dolci, 2019; FREED et al., 2019) use community-based participatory action research, to directly support survivors of technology-enabled intimate partner violence. Yet these kinds of research projects differ radically from the mainstream of cybersecurity research.

Cybersecurity research can discuss the "human factor" in ways that are at odds with theoretical and methodological advances in human-centred computing. Security research often focuses on defending companies or company property, with users portrayed as part of the problem.
A popular cybersecurity mantra claims that "humans are the weakest link" in cyber-defence strategies (McMahon, 2020). Research on "human factors" often focuses on "solving" what is perceived as risky internet behaviour such as choosing weak passwords or clicking on phishing links, often through workplace training and awareness courses (Hadlington, 2017). Many researchers in human-computer interaction (HCI), privacy-by-design and human-centred computing operate on the assumption that computer security can be achieved *with* users rather than despite them. Such approaches advocate for moving from "human-as-a-problem" to "human-as-a-solution" (Zimmermann & Renaud, 2019). This is reflected in moves towards "usable", "user-centred" and "human-centred" cybersecurity (Benenson et al., 2015b;

McKenna et al., 2015; Ramokapane et al., 2019; Whitten & Tygar, 1999b). However, research which sees humans as a solution still implicitly casts information systems (or organisations which own them), rather than the humans using them, as the "referent object" or the focus of protection (Ani et al., 2019).

Through using participatory methods, PTM aims to empower members of the public to improve their own cybersecurity practices and engage critically with the concept of cybersecurity. Rather than dictating what threats people *should* be worrying about, we develop a model for eliciting and listening to peoples' concerns to expand the scope of threat modelling. This is a useful approach because it offers a way to centre people's lived experiences rather than security experts' imagination of likely threat scenarios. Thus, participatory threat modelling works *with* people to determine what threats are relevant to their safety (rather than the safety of information systems.) The following section describes the iterative method through which participatory threat modelling was developed.

Methods & Process

This project originated in 2020 as a collaboration with Scarlet Dawson Duckworth, who, like me, had recently entered the field of cybersecurity with a background in political science and social science of internet technology. We wanted to challenge the perception of cybersecurity as an elite, inaccessible, and male-dominated domain among those traditionally excluded from cybersecurity design and implementation. With the help of my supervisor, Professor Gina Neff, we successfully applied for a UKRI Citizen Science grant (grant reference BB/T018593/1) with the initial aim of running 8 workshops from January to May 2020. We conducted the first four workshops in person, before the sudden escalation of the covid-19 pandemic and associated lockdowns in February 2020 delayed, extended, and hugely transformed the project. We extended the grant duration several times to 30 June 2021 (a period of 18 months rather than 5), with offshoots of the project continuing as I write this in November 2022.

As Pain et al (2010) note, participatory action research is more of an approach than a method: participatory threat modelling applies this approach to the method of threat modelling to develop a new method. As I described in Chapter 2, I use methodological experimentation and innovation as a form exploring and refining underlying concepts. This draws on critical security methods which engage in "a more free and experimental interplay between theory, methods and practice" (Aradau et al. 2014). Throughout several stages of this project, how we designed and conducted workshops changed, as did the nature of the partnerships on which they were based on. This section outlines these lessons and changes over various stages of the project, with a focus on reflections on the methodology and how we incorporated these reflections in

the iterative parts of the project. The choice to prioritise these reflections on the process is intentional, as reflexivity is key to the methodology of action research, and it is important not to present these reflections as an afterthought in a limitations section.

Our workshops started as self-contained interventions that created a safe space for participants to reflect on their online experiences and improve their digital privacy practices. In this first stage, we recruited members of "the general public" via fliers on community noticeboards, social media, and newsletters (see Appendix 1.2). Our recruitment materials emphasised that participants did not need any expertise to contribute beyond their experiences of online life. For some workshops, we partnered with community and activist groups including Extinction Rebellion Oxford, Victims of Image Crime, and People & Planet. These workshops allowed for more specificity as these groups had shared concerns.

Each workshop followed a similar format, starting with an introduction welcoming participants and outlining our motivations and goals (see Appendix 1.3). Next, we conducted a "threat modelling" session focusing on what participants wanted to protect in their online life, what made them feel threatened, and what parts of their digital security they wanted to improve. After that, we conducted a "tech support" session in which we pointed participants to online resources and worked with them to make practical changes. Our volunteer tech support staff were instructed to be caring and avoid "techsplaining or mansplaining" (see Figure 4: Tech support guidelines). Lastly, we facilitated a general discussion on the nature of and future directions for cybersecurity.

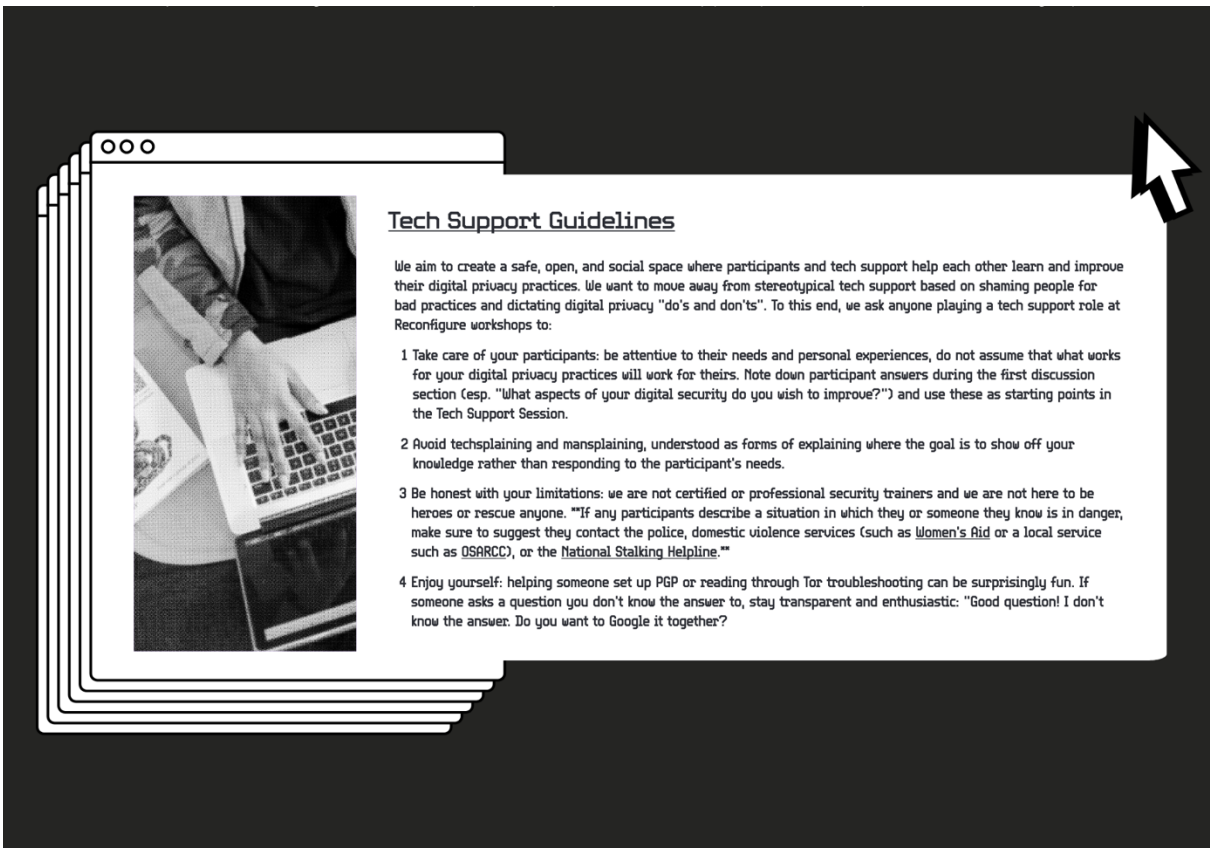

Figure 4: Tech support guidelines

In line with our feminist commitments (discussed earlier in Chapter 1), we aimed to create an environment of mutual care and support. Our questions focused on emotionality and personal experience—topics in which anyone's and everyone's answers would be valid. These methods reflect the theoretical commitments of the project, which see research as a form of intervention rather than a neutral data-collection exercise. The workshops were designed to co-create knowledge with our participants: for example, sharing participant responses on a screen throughout the workshop allowed people to comment and react to the contributions of others, creating a sense of communal sharing and debate.

To create safe spaces for discussion around sensitive topics, participating in the research aspect of the project was entirely optional. If the participants chose to opt-in, they could anonymously share their thoughts and stories on their own devices using the Mentimeter platform. Alternatively, participants could opt-in to recorded focus groups with the same questions. The first four workshops were held physically in the UK, with the rest taking place digitally due to the Covid-19 pandemic. With 10-12 participants per event, we had a total of approximately 90 participants in the first stage of the project. Follow-up interviews with seven participants explored their contributions in further depth.

After the first eight workshops, we analysed data we had collected and reflected on the method and findings. One thing which was clear from the early stages of the project is that participant recruitment strongly shaped the project. While the workshops were open to all, there was a high representation of women (65.6%) and non-binary people (9.8%).[10] Although our materials were inclusive to those who did not consider themselves "'tech-savvy"', due to our own environments, the nature of our partner organisations and the urban locations of the workshops, we found participants tended to come from relatively privileged educational backgrounds who were already somewhat comfortable with technology. We realised that to benefit marginalised communities disproportionately targeted by online surveillance and harassment, we would need to intentionally collaborate with them.

Second, we decided that the standalone quality of the workshops was a limitation, as many participants did not have enough time to both identify threats and implement solutions in one workshop. Third, as we did not collaborate with participants on the design of the workshops or on data analysis, our study was not fully participatory. In fact, I began to see the opportunities offered by grant funding increasingly as forms of restraint: as the grant had been initially formulated by a small group of two researchers and one technologist, the project was not conceived in a fully collaborative way. The grant reinforced an imperative to collect data and publish papers, which is prevalent in academic research, changing what started as a community-building project into a data-collecting exercise.

I wanted to incorporate these reflections in any future actions and saw an opportunity to do so in a collaboration with Voice of Domestic Workers (VoDW), a support group run by and for migrant domestic workers (MDWs) in the UK. VoDW helps MDWs leave abusive and exploitative employers as well as supports its members with immigration issues. This requires some further explanation on the specific situation of many domestic workers in the UK, explained in Figure 2. They also organise resources like English language and IT classes. VoDW was interested in taking part in our study because it had noticed an increase of digital privacy and security concerns among its members, particularly during the COVID-19 pandemic.

Figure 5: Migrant Domestic Workers in the UK

[10] These statistics are indicative rather than exhaustive, as all responses to questions were optional, and only about two thirds of participants answered this question.

Migrant domestic workers (MDWs) work in private households, usually as cleaners or nannies, and have moved from their countries of origin. Domestic workers are mainly women, disproportionately from ethnic minorities, and/or migrants (Gallotti, 2015). Despite the central role domestic workers play in responding to growing needs for care work, their work is devalued, and they receive inadequate protection from labour legislation (Sedacca, 2019).

MDWs are particularly subject to invasive surveillance both from the state (due to their immigration status) and in their workplace (as their workplace is their employer's home, giving the employer exemption from many labour rights). Privacy is often thought of within the context of protecting someone's home or personal space. However, when MDWs work inside someone else's home, they have little recourse to protection from employer surveillance (Sedacca 2019). Such digital surveillance practices can be harmful to both the employer and employee; for example, ethnographic research on Filipino MDWs in Hong Kong has shown that digital surveillance resulted in MDWs evading control and as a result not being able to deliver the best care (Johnson et al., 2020b).

In the UK, MDWs mainly enter the country with an Overseas Domestic Worker (ODW) visa (Kalayaan 2019; Home Office 2021), allowing MDWs to accompany or join an employer in the UK. The visa is valid for a maximum of six months with no right to renew or extend it. As of 2016, workers on an ODW visa can change employers but only during the six-month period. In practice, workers have little or no time left on their visa to find work. In exceptional cases, workers can extend their stay and work lawfully in the UK beyond the six-month period if identified as potential victims of trafficking or modern slavery. However, they need to wait months or even years for a decision to be made under the UK's National Referral Mechanism (NRM). During the waiting period (which for some MDWs has lasted as long as 37 months), many survivors are not given the right to work and, thus, are forced into informal and precarious labour, destitution, and exploitation (Sharp, n.d.). Like other aspects of the "hostile environment", these immigration policies by design make workers vulnerable to both on- and offline digital threats.

The UK's "hostile environment," a set of policies introduced in 2012 by the Home Office[11], aims to make it difficult for undocumented people to stay in the UK by compelling, for example, doctors, landlords, and police officers to check immigration status, which may result in migrants being denied access to essential services like the NHS, education, or reporting

[11] The Home Office is the lead government department for immigration and visas in the UK.

crime (Goodfellow, 2020; JCWI, 2020). The Home Office also has access to the data that public sector organisations use, such as patient health data, details of migrant victims and witnesses of crimes, or reports of unsafe working conditions and exploitative employers (JCWI, 2020). These policies harm all migrants and racialised minorities (Qureshi et al., 2020; Webber, 2019; Yeo, 2017) and have been widely criticised for creating "an illegal underclass of foreign, mainly ethnic minority workers and families who are highly vulnerable to exploitation and who have no access to the social and welfare safety net" (Yeo, 2017).

The collaboration with VoDW formed the second stage of this study, which addressed many of the limitations identified in the first stage.[12] Rather than working with the "general public", we were working with a very specific community with a shared identity and shared political goals (reinstating pre-2012 rights for domestic workers). Rather than running one-off workshops, we conducted four data collection workshops with different members of the same organisation, followed by a data-walkthrough workshop where we shared and received feedback on early stages of data analysis. We then created and disseminated a free online digital privacy and security guide, to make our research outputs accessible to the public as well as VoDW and several other organisations that protect migrant and precarious workers in the UK[13]. During each workshop, we asked participants whether they had any questions for us on online safety, privacy, and security. We noted down these questions as well as the threats participants had identified and their advice for other MDWs. We then used these as the basis of our online digital privacy and security guide, which we also presented back to the community in two dedicated privacy and security workshop focused on the guide (see Figure 6: social media content promoting our digital privacy guide).

[12] We were also joined at the privacy guide and paper writing stage by Mallika Balakrishnan, an organiser from Migrants Organise

[13] Accessible here: https://domesticworkerprivacy.github.io/

Figure 6: social media content promoting our digital privacy guide

Marissa Begonia, our peer researcher in VoDW helped organise workshops, develop the questions we asked our participants, and co-facilitated the discussions. I hoped this would ensure our study and research would be useful to the MDW community, however this deeper form of collaboration also opened up a new set of concerns around extractive research and potential harms to both participants and the organisation. There are many risks of potential harm in privacy and security research with at-risk populations, including a heightened need for confidentiality, consideration for possible past trauma, and research justice given inherent power differentials (Bhalerao et al., 2022). Although we took a variety of precautions against these risks (see Figure 7: Ethical concerns for MDW research project), ethical concerns beyond data anonymisation and reciprocity continued to worry me. As our funding only covered time spent *in* workshops, this meant any other peer researcher labour, including setting up workshops, paper writing or giving feedback on the paper and other project decisions was unpaid. Although there were areas where I wanted to have more input from Marissa to make sure that our research was aligned with her organisations' goals, I also felt like this would be demanding unpaid labour from someone whose time was already overstretched with important advocacy and support work. Furthermore, the fact that I had grant funding reinforced a power dynamic as I was paying both the peer researcher and participants.

Figure 7: Ethical concerns for MDW research project

Ethical concerns for this study included preserving the anonymity of vulnerable participants. We followed principles of data minimisation, ensuring that the research data that we

collected was not connected to participants' identities. To do this, we did not video or audio record workshops; we instead relied on handwritten notes which did not include participant names as well as used an online platform where participants could submit answers to our questions anonymously. Some participants also participated in the calls outside their home and workplace, e.g., in a park, to avoid being overheard by employers. Lastly, the only researchers with access to the personal/contact details of participants were those being involved in data collection and analysis. We also note that although some participants had experiences of being undocumented in the past (because of recruitment by our peer researcher), all participants had secure immigration status at the time of the study.

Another concern was the potential distress of participants who discussed difficult or sensitive experiences. To mitigate this, we reminded participants that they did not need to answer the questions, and they could take breaks during the study. Further, our peer-researcher at VoDW was present at all workshops to make sure that participants felt comfortable. Lastly, our research was reciprocal, to make sure participants benefited from the project, particularly as they belonged to a vulnerable group in often precarious employment. We made sure to compensate participants £50 for their time, and we attempted to ensure the accessibility of our research outputs through publishing a digital privacy and security guide online. This study was approved by the Research Ethics Committee at the University of Oxford.

Resources about participatory action research, such as Pain et al.'s (2010) questions for reflection, have been helpful for reflecting on and articulating these concerns. For example, I realised we organised meetings ad hoc and did not rotate facilitation of meetings, so I almost always took on an informal facilitating role which meant my views likely predominated over others'. Throughout the process, disagreements over the research process did not come up, but this could be a function of the fact that there was no clear framework for dealing with disagreement. These power dynamics can resemble a "tyranny of structurelessness" wherein a lack of explicit structure can disguise an informal, unacknowledged, and unaccountable leadership, which is enabled by a denial that the leadership exists (Freeman, 1972).

As Wolfson et al (2022) note, "when I think about research and research ethics, I always think through who I am accountable to, and through what mechanisms of accountability. If my research on social movements or labour struggles is not accountable to those struggles and is merely a function of my desire to publish, then the work is often extractive as opposed to symbiotic." We started the project with the ambition of organising as a non-hierarchical

feminist collective. But the grant we received imposed an immediate accountability to a funding body, which prioritised the needs and skills of academic researchers. I personally am accountable to the publishing requirements of an academic career, whereas formal accountability mechanisms to the participants and groups we worked with were unclear. Ironically, the extent to which I predominated over the research process is in some ways useful to me, as it means I can claim this as work that I was primarily responsible for (as I do in the Author statement) for the purposes of DPhil graduate research, a world where "individual achievement is rewarded" (Wolfson et al. 2022). However, this need for highlighting my own contributions is at odds with the principles of collaborative research and led to unnecessary distress caused by feeling personally responsible for research and publication decisions.

These worries persisted despite the many ethical precautions outlined above (which received institutional approval at the outset from the university's Research Ethics Committee and retrospectively from reviewers at the USENIX conference). Yet these precautions did not explicitly address power dynamics such as relying on unpaid labour of peer researchers. As in the paper we criticise the Home Office and the hostile environment, I worried about reputational risk or even attempts at retaliation. Due to my own positionality (class background, relatively secure immigration status, privileged education and the degree of protection offered by being part of the University of Oxford), I worried that any such harm would fall disproportionately on our peer researcher, research participants or the wider community of precarious and vulnerable people. These potential risks had to be weighed against potential benefits, such as reputational benefit for VoDW or a broader culture shift in security research towards supporting marginalised groups and community organisations. It was hard to tell which of these worries were reasonable, or necessary for me to personally feel responsible for. I did not feel qualified to be making these kinds of trade-offs, however discussing these concerns with my supervisors as well as with peer researchers at Voice of Domestic Workers and Migrants Organise was reassuring.

Ultimately, many of these concerns revolved around the project not being fully participatory: had peer researchers been involved in the earlier stages of project design and applying for funding, I would have felt more confident that the research is useful to the MDW community and in line with their needs and the risks they face. These are important learnings for understanding the kind of research I want to do in the future. I want research to be guided by principles of solidarity and coalition; a shared endeavour rather than saving, protecting, or speaking for vulnerable or disadvantaged groups (Dabiri, 2021; Hooks, 1986; Potts et al., 2022; Wolfson et al., 2022). As Mallika Balakrishnan, one of our peer researchers put it, "the closer we get to working in coalition, the more you can move from isolated hand wringing to communal

hand holding in the face of obstacles and risks." These reflections are important particularly as I am carrying over participatory methods into a discipline which does not usually use it. Due to the risk of "participatory" being applied as a gloss for ethics-washing or marketing your research, it is crucial to be very transparent with clearly specifying *what* the participation is and very honest with reflecting on power dynamics in research (L. Smith et al., 2010).

Tracing the evolution of the methods in this study from its origins as digital privacy workshops in local community spaces, to a yearlong collaboration with Voice of Domestic Workers and Migrants Organise, shows the importance of an iterative process with periods of action and reflection. Moving from ad hoc workshops with the "general public" and little follow up to iterative workshops with a specific community meant that we could model privacy and security needs and outline steps for action, resulting in a practical guide accessible to the community as well as an academic paper. From the beginning, we aimed to centre people rather than information systems in threat modelling. The messiness of the process highlights thorny questions of what it means to centre people in practice: which people? Individuals or groups? Where does the participants' voice end and the researchers' interpretation begin? How these methodological choices allowed us to identify more robust findings will be the focus of the next section.

Findings

The following section charts the findings from the first stage of the project through to the final collaboration with Voice of Domestic Workers. The first stage, i.e., one-off workshops with the public, resulted in a variety of interesting findings which demonstrated the value of threat modelling from multiple standpoints. Yet these findings were somewhat fragmented, due to the variety of people participating in each workshop. In contrast, the iterative project with VoDW resulted in a much more consolidated and focused threat model as well as a more concrete and specific set of recommendations to ensure security for migrant domestic workers.

Stage 1: Threat modelling with the public

The first stage of the project (standalone workshops with the public) generated a variety of novel and interesting observations. Participants perceived online threats in unique and unexpected ways, reflecting various social standpoints. Although many mentioned conventional cybersecurity threats such as password compromise and online banking as areas of concern, participants often reported being more concerned with reputational and interpersonal harms. These reputational concerns often tied into professional identities. Many participants learned about cybersecurity primarily in a work setting, and therefore their knowledge of company

policies preceded that of their personal cybersecurity. The need to maintain a professional reputation drove many participants' concerns for privacy, with “employers accessing old data” often mentioned as a threat. (P2,W7), who had been a sex worker noted that the security of her professional life was extremely important, but that she was often met with an attitude she characterized as “well you can’t expect privacy when you’ve done that sort of work.”

Many participants shared experiences of being condescended to, patronised, or subjected to ‘mansplaining’ due to their gender. Participants noted that people providing IT lessons or tech support are often male: (P3, W2) explained that “being a female getting tech support from a male can be disconcerting. Fears over what private info they might see, find, engage with … make women feel vulnerable.” This gendered vulnerability encompassed subjects from location-tracking, sending nudes to misogynistic trolling (particularly on Twitter).

Experiences of privilege (or lack thereof) linked to wealth, class, and education also shaped engagement with cybersecurity. Participants framed cybersecurity knowledge as a privilege that comes with good education. Being able to pay for technical or legal support (as well as tools such as VPNs) if necessary was cited as a big factor in limiting and enabling engagement online. Several participants hypothesized that their own privileged backgrounds had made them feel more complacent about security and privacy online. In contrast, several participants linked experiences of being in minoritized groups—due to race/ethnicity, sexuality, or gender identity, to a greater need for digital security. Participants who had been in organisations focusing on race, or just spoken out about race online, reported increased online aggression and worries about “doxxing”, a form of online harassment that “breaches perceived privacy boundaries by releasing information through online mass media channels, resulting in physical and online consequences for a target” (Eckert & Metzger-Riftkin, 2020).

Experiences of being queer and/or polyamorous online made people more aware of granular privacy settings which were necessary for “managing what I present to different audiences that have different levels of awareness of my sexuality” (P4, W2). This resonates with past research on virtual communities as safe spaces for LGBTQ youth to communicate and express themselves (Geeng et al. 2022; Lucero 2017a). (P5,I) outlined how online banking put them at risk as a trans person: as they live in a country in which changing your name to match your gender identity is not legal, their online banking still used their legal name, putting them at continual risk of being outed with each financial transaction.

Many of these threats—such as being outed as a trans or queer person, image-based sexual abuse, and misogynistic trolling—are not considered in existing cybersecurity threat models. These participants’ unique standpoints, informed by their lived experiences and varied

identities, contributed to a more robust understanding of both online threats and possible solutions. However, these threats lacked a certain specificity, as each participant shared their own worries which sometimes overlapped but often differed. Participants in these workshops had only met each other, and these workshops did not offer the time or space to identify shared concerns and develop solidarity around them (although participants did often recognise shared problems).

When we grouped people who shared similar experiences in a workshop, results became more nuanced and specific, as did the recommendations for change. For example, survivors of image-based sexual abuse faced a particularly challenging set of threats. Not only had they experienced ex-partners sharing intimate images online—including videos filmed without their consent—, but they also described ongoing harassment on social media as strangers continuously re-shared links to pornography sites which refused to take down these images and videos. This was reflected in their understanding of safety as "insulating myself and my community [...] from having to be exposed to things like this and educating people on how to create a safe bubble." Sharing a workshop with others with similar experiences was important as many of these survivors had not had an opportunity to speak to many other survivors of image-based sexual abuse. "This just occurred to me now on hearing you all speak, which, for me, [...] this was like third and fourth victims that I ever get to speak to. I feel that camaraderie, the solidarity—you understand just how deeply this—It really pretty much almost ruins your life for a period of time until it doesn't anymore." This camaraderie and solidarity were even more significant in the second phase of the project with Voice of Domestic Workers, a support group run by and for domestic workers.

Stage 2: Threat modelling with Voice of Domestic Workers

In the second phase of the process, workshops were done iteratively and with the same community, allowing for a much more focused exploration of threats, as well as a nuanced understanding of how various threats intersected to pose specific vulnerabilities. The process of creating a dedicated guide also highlighted the dangers of generic security advice.

Based on participants' answers, we identified three main categories of threats to MDWs: government surveillance, online scams and harassment, and employer monitoring. These concerns can fit together as a threat model, in which threats are ranked and reinforce each other, rather than an isolated list of concerns. In our data walkthrough workshop, we asked participants to rank the threats from the most to the least they were concerned about, which resulted in the order listed above. This was a surprising finding as we had expected participants to be most concerned about employer monitoring, which they had the most interaction with in

their daily lives. However, participants considered immigration surveillance and online harassment to be more serious threats. Consequently, we followed this prioritisation in our own analysis.

Government surveillance

The first category of threats refers to government monitoring of MDWs relating to their immigration status. Participants reported that public bodies such as the Disclosure and Barring Service (DBS) or the National Health Service (NHS) could be used by authorities to monitor and track MDWs and share their location and status with the Home Office, which made them feel concerned about their ability to work and access a general practice (GP). Three participants shared that they would like to learn about about government tracking from establishments such as DBS and NHS as part of the privacy and security guide for MDWs.

Participants explained that those who remained and worked in the country undocumented lived in fear of being found by such authorities (11). One participant shared that undocumented workers felt that they were being "chased after" by the stringent immigration system in the UK. One participant advised, "to those who don't have [the] right to work, turn off tracking, avoid video, don't put [any] exact [information about yourself]."

Even though participants had secure immigration status, proximity to others who might be undocumented meant that fear of Home Office monitoring was pervasive in their lives. A participant described how this affected them during the COVID-19 period: "[I] hesitated to get [a] COVID test because [I] was living with undocumented people and [I] don't want someone coming here to investigate." This experience highlighted that concerns about government tracking were applicable to all MDWs, whether undocumented or not, which further affected their access to healthcare.

Online scams and harassment

The second source of threat is online scams and harassment. Scams varied across different methodologies of fraud, such as identity theft (8), social media scams (7), mobile scams (3), and romance scams (2). Our participants often mentioned the need to stay alert to their surroundings as such threats were widely present across mediums (12); "I need to be alert to everyone else." Participants also reported frequent contact by scammers online and by phone: "calling me about accident, keep calling me same voice twice a week different countries."

Harassment based on gender or immigration status was also a concern that was raised by participants (8). Our peer researcher reported a case of "Zoom-bombing" in which a group of harassers infiltrated a Zoom meeting organised by VoDW to raise awareness of MDWs' need for

legal reform of visas. The harassers filled the chat and audio with racist and sexist abuse. One participant recalled a situation in which a man recruiting cleaners via Gumtree advertisements said "my girlfriend went back to the US, can you be my girlfriend? But also, my cleaner?" This reflected findings from past research on sex-for-rent ads on Gumtree, which identified the gendered affordances of seemingly neutral platform design (Schwartz & Neff, 2019). Most domestic workers are women [119], as are the participants for this research, which meant that they were more likely to experience sexual harassment and abuse both on- and offline. Another participant described a situation in which "you meet a guy, and we like to know each other, then he like to do more, we say no, men threaten today or tomorrow police will come to your place." In this way, precarious immigration status intersected with gendered vulnerability, so that "they look at vulnerability and use that to abuse you. Sometimes not just about sex but about money you're earning." These structural factors like gender and immigration status shaped how MDWs experienced safety and security online.

Employer monitoring

The third category of threats refers to how employers of domestic workers monitor their performance. Twenty workers reported having worked in a home with a CCTV camera or a similar monitoring device, while 7 reported they had not. There were divided opinions over employers' use of CCTVs for monitoring. Some participants argued these could be used to defend the house against intruders (4) or the workers themselves against false accusation (7), while others reported the cameras made them feel uncomfortable, nervous, or scared

(12). One participant recalled their experience working in a CCTV environment: "I saw it in my room and in the kitchen. It's visible. It can reduce violent attacks, and harassment and workplace theft." Another participant described a situation where this would particularly be useful for an employee being bullied by their employer: "[they can] slap and spit... [the] camera will know, [and we can] use it as [the] evidence."

On the other hand, others mentioned cases in which CCTV cameras were installed in intimate areas which made them feel invaded (3), highlighting the lack of respect and dignity that participants sometimes felt in their workplace: "I feel being not trusted and its weird that there's always an eye on me even I feel anxious if there's also in the bathroom?" These divided opinions partially explain why employer monitoring was not viewed by participants as the most concerning threat.

The purpose of technology use in employer's home was not always made clear to participants, who were left in the dark about how and when their camera data was collected. One participant described their experience working in ''a very high-tech house" which made them feel that their

voices could be heard by their employer all the time: “My employer have CCTV, hear our voice... They know what we’re talking about, they say ‘I hear you everywhere.’ ... she knows a guy asked my number. There’s some kind of gadget in laundry room. I asked what’s the purpose and they said it’s for music for both of you.” This suggests that the casual adoption of technology in the employer’s home could make it challenging for MDWs, who are on the other end of the power spectrum, to openly question a recording devices’ purpose and use.

As participants did not have direct control over the way the data was handled and stored, it was difficult to pinpoint whether camera recordings could benefit or harm participants.

One participant described being caught while escaping abusive employment due to CCTV cameras: “It’s like a trap, a cage. You see it as your weapon but it’s not really.” One’s data captured by employers might be used as proof against them especially in the case of family member exemptions[14]:“Photos on holiday, in cinema, eating with employer and family, can make you lose a court case due to the family member exemption.” The participant expressed how she did not perceive herself as a “family member” and that the “employer should treat [her] with respect and dignity.” Employers could also manipulate or delete data in their favour. One reported that “[an] employer can destroy [the data] unless the police gets there first” or enables access, implying how participants were aware of their lack of power over their own data.

Our findings also indicated that a lack of privacy was not limited to digital spaces. Participants generally experienced high levels of non-technical surveillance as well, with two participants saying that the situation was worse when “the children are the camera” because parents teach their children to report on domestic workers and “children can make stories.” Participants also discussed the fact that they had limited physical privacy and, thus, very little time to use their phones. One participant recalled that one family she had worked for had strict rules about using a phone: “Phone is not allowed there. So I need to hide it in the back of the toilet bowl. So if I go for a shower at night, I can message my family.” The founder of VoDW also expressed similar points, noting that the bathroom was “the only room with lock and with no camera where we feel safer against our male employers.”

The bathroom simultaneously offered MDWs a space of physical privacy, without CCTV surveillance, and allowed them the chance to connect digitally. A combined lack of physical privacy and lack of privacy online leads to a pervasive sense of being watched. These anecdotes

[14] See (Sedacca 2022) for a discussion of these legal loopholes which allow employers to avoid minimum wage requirements through claiming a domestic workers is a familing member

also emphasise how little personal time the MDWs we spoke to had, which is a serious consideration for digital privacy and educating oneself on privacy settings.

The three categories of threats described above are interconnected and reinforcing, as is evident in the case of dating abuse where men will threaten to report workers to immigration authorities. Precarious immigration status makes workers fundamentally vulnerable to other threats like online scams and interpersonal abuse from partners or neighbours.

Impact and harms

This section explores how the identified threats affected participants. Participants noted that their experiences online had led to a lack of trust in others and in the institutions that monitored them (23); many of the MDWs we spoke to said it was "really hard for me to trust anyone. That's why I don't go out." This fear and mistrust permeated everyday life and made it harder to form friendships and relationships in their new country (6).

It was particularly pronounced in online interactions: workers described mistrusting messages from strangers and even from family members, feeling they might be subject to scams or identity theft (5). This was particularly damaging given the centrality of digital technology and social media for contact with family abroad. One participant described changing her name on Facebook and hiding information about her workplace on her profile because "people can take advantage of your situation"; someone who knew where she worked could report her to the Home Office. Participants described how fear of being reported to the Home Office as a form of retaliation or as part of accessing social support impacted their day-to-day lives negatively (6). For example, one worker noted that "in the flat I'm renting if there's ever a fight, maybe she will report to immigration. Being undocumented, if you're socialising with anyone, you have to be humble, don't be boastful or arrogant so they don't report you."

Scammers and other malicious actors were able to harm participants due to hostile environment policies which turn day-to-day public services into sites that could be used for detention and deportation, leaving uncertainty and low public trust in places of accessible support. The impact of many of these harms was worse because workers had limited social support and serious reservations about accessing services like the NHS and the police. An undocumented worker, who is fearful of being found by government authorities, would be less likely than a documented one to seek external help for their situation. This made them particularly vulnerable to scammers – something that several workers were aware of and noted, remarking that "hackers" could "use [their] status" (2).

The precarity of the worker status also sheds light on dependent relationships among workers themselves. For example, one workshop participant, who lived alongside other MDWs, noted that they were "not that strict," but that they told workers to "be careful because if they get in trouble, I get in trouble. [I'm] not trying to control them." When the workers live with someone else who might have more precarious immigration status, their living situation obliges them to be conscious about not only their own safety but also that of others. Therefore, worker's understandings of safety and security were highly relational, as we describe in the next section.

Although the community was clearly valued for the positive impact it could have on wellbeing and security, many domestic workers we spoke to still seemed to feel responsible for themselves and often used language to suggest that no one else could protect them (5). The lack of trust in systems, employers, and institutions manifested itself in loneliness and isolation from society, as well as potential health impacts due to fear of accessing health services.

Sources of safety

In her study of threat modelling with civil society groups, Kazansky (2021) notes concerns that the negative focus of "threat modelling" might be overwhelming to marginalised groups facing multiple threats (like MDWs); therefore, it is critical to also focus on existing sources of strength to build on. This section describes the actions that MDWs had previously taken to address their concerns, and further changes which were necessary to ensure a safer environment for MDWs. Sources of safety identified by participants can be categorised into three broad themes: 1) a sense of community, 2) control and knowledge about "keeping yourself safe", and 3) advocacy for legal reform and structural change that is necessary for meaningful safety.

Sense of community

Sense of community was a key element that helped participants navigate the aforementioned threats and negative impacts. Several participants reported that VoDW was their main community that they considered as family (6). One participant dedicated their ability to thrive as a domestic worker to the organisation: "Having a community, a family here in the UK is very helpful to us... because [being] away from the family is a challenge for us... They will look after you, and give you, not only financial matters, [but also] emotional and spiritual [aid] and everything you will [need] to survive. You will pass all the challenges with the help of the community, which is the biggest help for me."

As a result of the inability to trust people from outside, the MDW community formed a strong 'in-group' that filled gaps in support. Membership in this community also carried a corresponding sense of obligation, with one participant saying, "each one of us has the

responsibility to look after each other. ...we are responsible for the whole community." In the absence of care from family members, who were usually not in the country, or from the government, which many participants described with fear, the MDW community often practiced regular care towards each other. Although VoDW is primarily concerned with providing immigration support and advice on visas, the organisation also educates and advises MDWs on digital privacy issues and digital literacy.

Social media also enabled workers to reach out and maintain contact with those that made them feel part of the community; according to one participant, "It's comfortable [because] through social media I can keep in touch my relatives [and] friends that in far country." This was particularly useful given the international background of the workers: "I feel good by using social media because of social media we are now able to interact with thousands people all over the world this is why we see people who have thousands of Facebook friends." Another participant added, "I feel confident using social media, because I can communicate with my family back home and find any information I need." However, as discussed earlier, this conversely also made MDWs more vulnerable to scams and harassment on social media.

Control and knowledge

Many MDWs we spoke to also described the importance of "keeping [myself] safe"; i.e., the importance of looking out for oneself. Participants emphasised the importance of keeping personal details private and to not put personal information on social media (12), particularly information about financial success (1).

Participants offered insights into the way workers can keep themselves safe online; for example, according to one participant, "my simple advice that I can give to the other migrant workers to stay safe online, please think twice before going to unsafe websites, put strong password[s] and do not store a lot of personal info online. Also don't reply [to] messages from people they don't know." The popular consensus among participants (8) was to enable the settings in a way that they could decrease the chances of strangers with malicious intent: "Use private so that no one will connect me, like people I don't know." Several showed detailed knowledge such as limiting location-sharing and access by "friends of friends." Many participants also expressed enthusiasm about learning more about online privacy, and participants asked us several questions relating to this, e.g., one participant asked if it was risky to charge one's phone at the airport while another asked for more information on what to do if they became a victim of an online scam.

Knowledge was important to facilitate a sense of safety. Participants (8) reported the significance of being aware of CCTV locations in their sense of safety and dignity: "the

CCTV camera is on the door, you know the aisle, the door, not on the bedrooms... on where people get into the house and contents that surround the house. Not on inside. For me [this is] very important." Personal devices such as phones were used to enhance their awareness: "it's very important for us to know where the cameras are. Actually, for my current job, all their CCTVs, I have access on my phone. So... when the door rings I have access, I can see who is outside through my phone." While it was rare that participants had personal access to CCTV footage in this way, this participant reported much more trust and satisfaction with her employer as a result. Some participants were even vocal about their rights to privacy and the need to draw a boundary where CCTVs were no longer acceptable: "they (the employers) told us they will put [a] camera... [but I said] not near [the] bedroom. I said 'that's my privacy. Don't they dare.'"

Legal reform and structural change.

When asked what kinds of support they needed to stay safe, some workers specifically called for reinstating "the pre-2012 rights for domestic workers" (3). These rights would allow them to renew their visas and to ensure there is a route to settlement. One participant said that "if we have right to renew visa and work freely, socialise without fear, you can work freely, and employer cannot touch you and cannot threaten you. There's no burden on your shoulder." The current visa regime creates unnecessary precarity which opens up MDWs to a variety of on- and offline abuses from their employers, people in their social circles, and law enforcement. This has a direct impact on digital privacy and security. For example, it is easier for a worker to confront their employer about surveillance if that worker has more secure employment and immigration status.

This finding differs from previous security research with migrants in the US, which found that "their understanding of government surveillance risks is vague and met with resignation" (Simko et al., 2018). This may reflect the politicised nature of VoDW, which organises campaigns for legal and structural reform, and illustrate potential risks with universalising different migrant people's experience across different countries, nationalities, and legal situations. There may be significant variation even within any group of people, and qualitative research often does not aim for generalisation. These repeat calls for reform also reflect how fundamental these legal regimes are to workers' safety; no analysis of MDWs' online safety would be complete without considering immigration regimes which impact every other aspect of their working and private lives.

The government and employers must take responsibility for protecting workers' privacy and safety. The government needs to improve work conditions in the UK, create a safe environment,

and protect workers' human rights. Employers need to understand domestic workers' right to privacy and safety, and refrain from excessive monitoring.

Although participants had a strong understanding of what kind of legal reform of immigration rules was needed, they were less clear on how laws governing digital technologies could protect them. For example, when we asked participants if they had questions for us, one participant asked, "Is it legal to record workers in your home? Is it an invasion of privacy?" To answer this question, we realised that the UK law on CCTV recording in the home is both complex and ambiguous[15].

Like employment laws, in data protection laws the right to privacy of a family is often used as an exemption from protection that workers need (ILO C189). CCTV installations in privately-owned homes are legal if CCTV cameras do not record those outside the property (ICO n.d.). Yet, it is unclear what this means for domestic workers, who often face pervasive and sometimes covert surveillance. Under the UK Data Protection Act, covert surveillance is only lawful if the person recording has genuine suspicions of criminal activity. Covert surveillance must be strictly targeted at gathering evidence linked to that activity and cannot go beyond what is necessary for the investigation (ICO n.d.).

The most available sources of information online are websites for employers from nanny agencies[16] or surveillance equipment vendors[17] on "how to keep a legal eye on your babysitter." These have sometimes contradictory information which seems dubious.

Moreover, even when a clear violation (e.g., covert surveillance in private spaces such as bedrooms or bathrooms) occurs, it is not clear what recourse to justice workers may have. The ambiguous nature of current laws overseeing migrant workers result in inconsistent interpretation of one's status and rights, forming a root cause for constant insecurity to the workers. In our digital privacy and security guide, we point to legal bodies that can support workers when subject to the aforementioned threats or harms. However, these are highly context-specific, and may be complex and costly to workers themselves. Our work sheds light on the fundamental need for supporting MDWs' digital privacy and security not only in technology design but also through legal and employment rights.

---

[15] We asked participants if they had any questions for us during the workshops. Their questions and our (desk-based) research to answer these questions were part of PTM. This explains why we present as part of our findings both the participant's question and our research on UK data protection law to answer that question.

[16] https://www.elitenannycompany.co.uk/ trusting-your-nanny-to-nanny-cam-or-not/

[17] https://www.spyequipmentuk.co.uk/ how-to-keep-a-legal-eye-on-your-babysitter/

UK law on indoor surveillance devices needs more clarity regarding workers whose workplace is in someone else's household. There needs to be a clear prohibition of covert, non-consensual surveillance of domestic workers, and clear routes for restitution in cases of invasive recording or unnecessary data-sharing. Laws to regulate or even ban covert surveillance devices would also help curtail abusive use of these technologies.

Lastly, creating safe conditions for MDWs will require ending hostile environment policies: the hostile environment tries to make the UK inhospitable for undocumented migrants, ultimately creating violent and discriminatory realities for all migrants as well as people of colour.

Data sharing across different and unrelated government institutions, such as the Home Office and the NHS, is a major barrier to MDWs feeling safe and being comfortable accessing healthcare. Similarly, police sharing data of victims of crime with immigration enforcement can leave migrants fearful to report abuse. As an intermediary step to ending the hostile environment, we call for data sharing firewalls between immigration enforcement and data systems for healthcare and reporting crimes. MDWs in the UK should be able to access healthcare freely through a truly universal NHS, regardless of citizenship and immigration status.

In contrast with the first stage of research, our workshops with VoDW demonstrated a community-based approach to security. Although the first stage of workshops at times successfully created a community atmosphere, working with an existing community with strong support networks demonstrated the strength of building on a shared standpoint. MDW's experiences of (in)security came through more clearly both due to the iterative nature of the workshops, and because they shared so many experiences. This does not mean necessarily that one format for PTM (iterative workshops with one community) is "better" than another (one-off workshops with the public), however the differences between workshops do demonstrate the complexity of how *who* participates and *how* they participate can change the findings.

Discussion

In this section, I highlight three key methodological, empirical, and theoretical contributions from this study: first, I identify the overall strengths and promise of the method of PTM for security research. Second, I outline how the threat models elicited in the study contribute to our growing understanding of how marginalised groups experience specific and intersecting security challenges. Lastly, I demonstrate how standpoint epistemology produces a different understanding of where security comes from, resulting in a call to action for security researchers to apply this method and practice a different kind of security.

Methodological: participatory threat modelling

The method of PTM allows researchers to collaborate with members of the public or specific community groups in the process of problem definition (which underlies the security method of threat modelling). As discussed in Section 2 (Problematising Threat Modelling), in many studies in which participatory action research has been used in technology research, a solution—i.e., involving community members in the deployment of a new technology—is implicit in the study design. Creating spaces for reflection on existing technology use can also more valuable than framing research around developing a new technical solution (Strohmayer et al., 2019). In this project, asking participants "what makes you feel unsafe online?" rather than "how can technology be built more safely?" allowed for a more open-ended discussion of technology-mediated threats (such as Home Office surveillance) which are unlikely to be resolved through building safer technology. Therefore, PTM offers a way to escape the technological solutionism inherent in the majority of technology research (and not only PAR studies) (Morozov, 2013). In. contrast, such threats would have never occurred within the scope of the threat modelling done in Chapter 3, which was limited by a specific system (smart home devices) and therefore could never have included Home Office surveillance of medical records.

In workshops with the public, we asked participants what cybersecurity tools they needed or wanted. Participants sought simpler, user-centred, intuitive tools such as an "erase me button" that might to delete their data from any given website or regularly prompts to update their privacy settings. But many participants consciously resisted the notion that they needed new tools, instead raising the need for different norms around cybersecurity. (P7, W3) wrote "tech worlds encourage tech solutions, but I don't want more complex tech/ [or to] buy more tools."

Developing the digital privacy and security guide in collaboration with our participants helped us identify gaps in existing support and ambiguities in current legal systems that make domestic workers more vulnerable. In this way, the process of putting together a guide unearths areas where research, reform, or more information is needed in a process that combines action and research. This follows calls from past research for "community-appropriate educational resources" (Guberek et al., 2018). The participatory action research approach, including cycles of action and reflection and combining activism and research, could be used to develop further security resources for groups that experience multiple forms of marginalisation. This also creates a pragmatic resource with a direct benefit for MDWs. As our peer researcher has put it, "I hope in the long term, Voice of Domestic Workers can use this to educate MDWs and others to

better protect themselves on-line because many domestic workers are turning to social media as their way to ease their isolation and vulnerability."

However, solutions like the guide, which can contribute to the knowledge and resources that MDWs have to keep themselves safe, may also have the unfortunate effect of transferring the burden of "safety work" (Harris & Woodlock, 2019) on to those already burdened by precarity and abuse. Therefore, legal change and structural reform are also necessary for meaningful safety.

Participants felt individual users should not be held responsible for learning about cybersecurity developments. Many participants reflected positively on the communal nature of our workshops, and called for similar coordinated, community-based responses which go beyond technically oriented solutions that can contribute to cognitive overload and alienation. As (P8, I) described it, the "atmosphere we had in the workshop" helped create "confidence in hearing various tech terms and not being scared by them as such." The notion of 'group privacy', which was continually raised by participants, suggested security for the individual improved that of the collective, and vice versa (I return to this in the final section on theoretical contributions).

Applying the approach of PAR to threat modelling is not meant to replace conventional techniques such as asset-based or attack-based threat modelling. Rather, it expands the perspective of threat modelling in a way that should help security researchers prioritise threats which affect marginalised people, which historically have often been excluded from security research. PTM offers a way for researchers to identify problems that are grounded in marginalised groups' experiences rather than those of security researchers. As I noted in my reflections (in the Methods & Process section), this involves navigating the power dynamics inherent in any research. Careful attention to these dynamics and positionality in the research process is necessary to move towards solidarity rather than saviourism. In this way, methodological experimentation and innovation were also a form of exploring underlying concepts like security, care, and solidarity, in line with critical security methods (Aradau, 2014).

Empirical: threat modelling from a standpoint

If done with care, PTM offers a way to incorporate the power imbalances and centre marginalised peoples' experiences in security research. By asking participants to define their own threats, we developed a more robust threat model than we would have if we had pre-determined a single threat actor (e.g., employer surveillance) or technology (e.g., smart homes devices) to focus on. This also allowed us to map how different forms of threat reinforce each other. PTM shows that different groups of people have different threat models, affecting how

they perceive threats, how they define generic concepts like online safety, privacy, security, and what methods and mechanisms they employ to defend against those perceived threats. Future research should seek to further distil and differentiate to determine the needs of different groups, particularly marginalised communities. This can also involve thinking about the different regional, cultural, and geographic issues each community might face.

Which people are involved in threat modelling significantly alters both what is perceived and prioritised as a threat and where people look to for security. While some participants in workshops with the public reported a kind of complacency around digital privacy, which they associated with relative privilege and social security, those who had been targeted by indiscriminate cybersecurity attacks or targeted attacks based on identity were much more motivated to care about privacy and security.

This was consolidated in the second phase of research: migrant domestic workers' threat prioritisation reflects the different impacts of surveillance on people with different social and legal statuses. Past research on native domestic workers (Bernd et al. 2020) has documented how the fear of losing jobs stopped domestic workers from being able to negotiate CCTV camera use. MDWs both share these concerns of precarious workers and must worry about the risk of being reported and deported, even for some who entered the country using a legal route and then experienced labour exploitation or abusive employers. Furthermore, losing a job can in some circumstances lead to losing legal status if you cannot find a new employer.

Therefore, security researchers need to address the relationship between digital security and political phenomena, such as the hostile environment, fomenting conditions for high levels of security risk. Given that immigration policies (and technology, for that matter) do not exist in a vacuum, our research highlights that the digital security risks created by the hostile environment play out in the lives of MDWs through distinctly gendered and racialised forms that are further inflected by the labour precarity characterising domestic work in the UK. Labour precarity, immigration enforcement, and targeted, gendered violence all intertwine to create a set of digital security threats which the literature currently neglects.

Theoretical: threats as structural, security as communal

In this section, I return to my conceptual framework of reconfiguring cybersecurity. Threat modelling with marginalised people points to structural insecurity caused by oppression. Where conventional cybersecurity frameworks, such as the "CIA model", focus security practices on technical vulnerabilities and fixes, participatory threat modelling (which offers a method for reconfiguring cybersecurity) can refocus security practices to bolstering community

support networks and dismantling oppressive systems. Therefore, this final section outlines a different concept of security, intertwined with a call for a different kind of security research.

Our findings highlight the imperative for privacy and security literature to consider intersecting forms of marginalisation (due in part to different levels of social and economic power) and the broader social structures that create insecurity. In doing so, we respond to calls to "discuss the value of intersectionality as a framework for understanding vulnerability to harms in security research" (Geeng et al., 2022). Not doing so leaves key vulnerabilities and threats unaddressed and functionally contributes to the further marginalisation of people disproportionately impacted by those threats like MDWs. This resonates with security research on refugees, finding that online scams target people's specific vulnerabilities (Simko et al., 2018).

Inclusion of the threats that marginalised communities disproportionately face is a first step towards an ability to analyse and address these threats. Digital security researchers should also expand our methodological approaches to clearly address the direct relationship between oppressive socio-political structures and resulting digital insecurities. To do this, technical approaches are necessary but insufficient; non-technical interventions are also needed. This resonates with research on undocumented migrants (Guberek et al., 2018) and queer people (Geeng et al., 2022), which found that research on marginalised groups often results in recommendations for structural changes to best protect their users. This is not only a methodological point but also an epistemic one: who gets to define threats in security research changes not only the content of security recommendations but also the underlying concept of security that is contained in them.

In the first stage of research, many participants suggested structural changes were needed at the level of culture and legislation to improve the safety of our digital 'streets.' As (P9,I) put it: "all these potential tools hinge around the fact that what you really want is [...] trust. Like if someone could just invent […] some way of definitely holding Facebook [or] Instagram accountable." However, these findings on structural reform tended to be general and vague. When asked what they would have wanted to learn more about, several participants mentioned the socio-economic aspects of data collection, such as how it creates profits for businesses. Later workshops could build on this reflection by focusing less on individual actions and tool-based solutions, and more on developing community and finding structural solutions, reflecting the shift from "digital self-defence to data politics" (Kazansky 2021). Akiwowo (2020b) develops similar notions of "digital self care" and "digital citizenship" to articulate the relationship between individual and societal responsibility for online safety.

The themes of group privacy and community security were consolidated in the second phase of the study: as a community, MDWs were clear that legal reform was a necessary change they needed to be safe online, and had clear recommendations for what this legal reform should look like (described in detail in the final part of the Findings). Similarly, when brought together with other survivors of image-based sexual abuse, survivors had clear ideas both for legal reform and changes in technology. The method of participatory threat modelling also helped us identify further areas which needed reforms, such as UK law on surveillance devices.

However, in the absence of state protection, many of the most significant sources of safety in MDWs' lives are not necessarily technical but social and communal membership in community support networks. Our participants often described both vulnerability and security in social/communal forms, i.e., a risk to one person often extended to threaten more than just that person. This highlights that individualistic models of vulnerability and security do not sufficiently capture the real-world experience of these concepts. In a situation where MDWs often cannot trust others, especially online, participation in VoDW became a way of creating security for themselves and each other. This resonates with similar findings based on research with activists, refugees, sex workers and queer people, demonstrating the importance of community support groups and collective security (Albrecht et al. 2021; Simko et al. 2018; Strohmayer, et al. 2019; Geeng et al. 2022).

Politically contextualised analysis also offers security researchers insights into the conceptual tools we use and assumptions we make. For example, our findings show that both security design and privacy laws favour homeowners as the relevant subjects in cases where domestic workers are "guests" or "bystanders." What implications and insights might result from disrupting this norm?

Past research with survivors of intimate partner violence has shown the importance of robust multi-user security and privacy controls and designing surveillance devices to make it more obvious when they are on through visual or auditory clues (Leitão, 2019). Crucially, such configurations should not only prioritise the home or device owner. Existing literature discusses use cases like "only allowing guests and domestic workers to access smart home devices while in the house" (Zeng et al., 2017). However, the findings we reported on CCTV data ownership show that domestic workers may need to use footage to document abuse. This would likely only be possible if workers can access this footage once they have left the physical premises of the house, perhaps because they left exploitative employment. Access control policies and mechanisms should include the possibility of sharing data with domestic workers

and other guests in the house by e.g., giving them access to footage that was recorded while they were physically in the house.

In line with past findings (Bernd et al., 2020; Johnson et al., 2020), we found that our MDW participants were very uneasy with the existence of secret recording devices. Device manufacturers should not produce cameras and other surveillance devices meant to be hidden for the consumer market, as such devices are particularly likely to be used in ways which are unethical and abusive. Features like blinking lights which indicate recording can help make surveillance more transparent to all stakeholders in the household.

Some employers may not be intentionally malicious but may participate in use cases that are abusive. As a result, product packaging and notifications, particularly during installation, could nudge owners of devices towards following important norms. For example, CCTV cameras or nanny monitors could remind users these devices should not be in private or intimate places like bedrooms or bathrooms, informing them that this is illegal as well as unethical. Similarly, they could remind users to inform other people in the house about the recording device and prompt them to ask for consent before recording others. This might increase transparency and ethical behaviour, which in turn improves workplace and home relationships. Future research should explore the efficacy of nudging users towards ethical behaviour towards others in the household or at least abstaining from unethical behaviour, particularly regarding surveillance.

Use cases which solely consider homeowners' safety ignore the needs, vulnerabilities, and rights of other people in the house who are affected by technology use. They also reflect assumptions made by security researchers about who is a threat and who should be defended. These assumptions in turn reflect the positionality of the researchers making these assumptions and can be challenged through collaboration with those from different social standpoints.

Lastly, security research often supports the development of surveillance technologies in an attempt to prevent harms. Our findings highlight a need for a shift in the attitude of security researchers towards these technologies. Our work highlights the indisputable harms that those surveillance technologies enable in the lives of marginalised groups, which has already been championed by groups like No Tech for Tyrants.[18] We argue security researchers must consider and seriously weigh the impacts that the development of surveillance technology may have on the most marginalised people. As such, we call on security researchers to avoid developing surveillance systems and collaborating with border enforcement.

[18] https://notechfortyrants.org/

Conclusion

PTM uses feminist participatory methods to centre people's concerns instead of the integrity of information systems, which is the central component of my reconfiguring of cybersecurity. Applying the approach of PAR is not meant to replace conventional threat modelling techniques but rather to expand threat modelling to include and prioritise threats which historically have often been excluded from security research. My results illustrate what security which is grounded in people's concerns looks like: i.e., messy, contingent, and impossible to disentangle from politics, social norms, and other areas which technical security researchers often wish to compartmentalise as beyond the scope of their profession.

The two stages of the study illustrated two different modes of participatory threat modelling. The first stage illustrated the benefit of threat modelling from a standpoint and pointed to security solutions beyond new tools, but the one-off nature of workshops and the open recruitment method resulted in a lack of specificity in findings. In contrast, using the method of PTM in collaboration with migrant domestic workers, we defined a robust threat model for MDWs, which includes intertwined and reinforcing threats from immigration surveillance, online scams and harassment, and employer monitoring. It also showed precisely how these threats intersect: user privacy and safety are exacerbated by existing offline societal issues, such as immigration policy. This broader understanding of security invites a reframing, or reconfiguring, of the role of the security researcher: not only to build safter technology, but also to join those who are challenging unjust power structures to dismantle the structures—like the hostile environment and pervasive surveillance—that create insecurity. Such collaborations pose both thorny problems and great opportunities: reflections on the project echo previous calls for solidarity with an awareness of positionality. But first, do no harm: security research must seriously reconsider its role in facilitating the development of surveillance systems in the first place.

These workshops did not merely result in academic research which names threats and recommends solutions (although this is valuable), they also resulted in engaged actions such as tech support sessions and a pragmatic resource for participants. This is a model for more grounded and engaged security research: through our recommendations, we call on the security community to support local community support networks in coalition and solidarity. In the next chapter, I explore in further depth the "networks of care" which support organisations create beyond state and corporate security. We must collaborate with these networks and marginalised groups when designing information security frameworks and legal guidelines to

ensure no one is left behind. As our peer researcher, Marissa Begonia, wrote: “Instead of becoming victims trapped in hidden surveillance, communities such as those of MDWs can be active participants in creating a safer digital world.”

Chapter 5: Networks of Care[19]

Chapter summary

As technology becomes an enabler of relationship abuse and coercive control, advocates who support survivors develop digital security practices to counter this. Existing research on technology-related abuse has primarily focused on describing the dynamics of abuse and developing solutions for this problem; I extend this literature by focusing on the security practices of advocates working "on the ground", i.e., in intimate partner violence shelters and other support services. I present findings from 26 semi-structured interviews and a data walkthrough workshop in which advocates described how they support survivors. I identified a variety of intertwined emotional and technical support practices, including establishing trust, safety planning, empowerment, demystification, supporting evidence collection and making referrals. By building relationships with other services and stakeholders, advocates also develop networks of care throughout society to create more supportive environments for survivors. Using critical and feminist theories, I see advocates as sources of crucial technical expertise to reduce this kind of violence in the future. Security and privacy researchers can build on and develop these networks of care by employing participatory methods and expanding threat modelling to account for interpersonal harms like coercive control and structural forms of discrimination such as misogyny and racism.

Introduction

In the past two chapters, I presented two methodological innovations which reconfigure cybersecurity methods to better respond to problems of tech-enabled abuse. In this final

---

[1919] Author statement: this chapter was written based on a paper titled "Networks of Care: Tech Abuse Advocates' Digital Security Practices" which I co-authored with Dr. Angelika Strohmayer and has been accepted to the '22 USENIX Security Symposium. As first author, I was responsible for overall research design, participant selection and recruitment for the interviews, interviewing all participants, initial data analysis and coding, and writing the majority of the paper. Together with Dr. Strohmayer, I organised a data walkthrough workshop with some participants in this project, where we collaborated on recruitment, workshop organising, and facilitating. Dr. Strohmayer was responsible for data analysis from this workshop, writing parts of the Introduction, Methods and Conclusion of the paper, and securing a grant which funded part of this workshop and my work as an RA on the project. For this chapter, I amended sections of the paper, removing the background and literature review (which is broadly repetitive of Chapter 1), and expanding on our methods in greater detail than conference paper limits allow.

chapter, I look at a case study of feminist cybersecurity "in the field": i.e., cybersecurity support practices among advocates who support survivors of coercive control, sexual violence, and intimate partner violence. Advocates and support organisations have developed strategies that counter tech abuse and support survivors in developing digital safety practices.

As discussed in Chapter 1, security researchers have started to discuss technology-enabled abuse in intimate relationships and other forms of coercive control. For example, many researchers (both within and outside of security studies) have (1) built an understanding of the dynamics of tech abuse and (2) developed solutions that aim to reduce this kind of violence. Both kinds of work often jump to conclusions about what security researchers, developers, or designers can do to tackle this issue. The first two studies of this thesis recreate this tendency, by seeking to develop new responses to the problem of tech-enabled abuse. However, we seldom examine what is already going on outside our field to learn from the expertise of those who have been doing this work for a long time. With this chapter, we counter this tendency and instead bring lenses of care and empowerment into security discourse based on the security work of advocates who support victim-survivors[20] of tech abuse.

This chapter responds to the need for more nuanced empirical work on existing security practices in the context of services for survivors of coercive control. In doing so, we contribute to privacy and security research in three ways: (1) we expand the field's understanding of technical support by highlighting the ways it is intertwined with emotional and psychological support; (2) using critical and feminist theories, we question conventional understandings of security by adding the notion of networked care and relationship-building as integral to the work of security experts; and (3) we redefine technical expertise in security, including knowledge from experiences of on-the-ground support workers and advocates. Networks of care are networks of practitioners willing and able to support survivors with specific needs. Developing and maintaining these networks is a critical security practice that advocates do to create more supportive and caring environments for survivors—a process similar to feminist activism against gender-based violence which works to create safe(r) spaces. By understanding the practices of these "networks of care", security research can learn how to build on and expand existing support systems, rather than parachuting in new solutions which ignore or even interfere with existing support networks. These theoretical shifts have immediate

[20] We use this terminology as a way of being inclusive in our language. It is a phrase used in violence research to account for peoples' diverse experiences of violence - some may prefer the term victim while others prefer the term survivor as people may be uncomfortable with either

implications for privacy and security research, such as a need for more participatory research with practitioners who support survivors of violence and expanding threat modelling to include interpersonal harms like coercive control and structural forms of discrimination such as misogyny and racism.

Below, we present our research methods, including information about our participants and our standpoints as researchers. Following this, we present our findings related to existing support practices, the importance of understanding care as a network, and detail the recommendations for change needed in security technologies and practices that advocates have outlined in the interviews. We conclude with implications for privacy and security research.

Methods

In this chapter, we expand research related to technology-mediated abuse by learning with and from safety advocates using semi-structured interviews and participatory forms of data analysis. Our research is underpinned by a feminist framing of safety and digitally mediated abuse which involves centring our participants' expertise not just as 'advocates' but also as security experts. Below, we first present details on our interviews and analysis before addressing the issue of positionality in our work.

Qualitative interviews

To explore advocates' experiences of supporting survivors of technology abuse in depth, we conducted 26 semi-structured qualitative interviews (see table below), each lasting one to two hours. Most participants (22/26) worked in the gender-based violence (GBV) sector broadly construed, i.e., organisations with a focus on intimate partner violence, family violence, human trafficking, and sexual violence. A few participants (4/26) came from digital privacy groups or hacking collectives which had begun to support survivors of intimate partner violence as a part of their advocacy, often as volunteers. Advocates had worked in the domestic or sexual violence sector for an average of 9.2 years. Lastly, several participants were specifically recruited because they support communities like sex workers, refugees, or LGBTQ+ people who are sometimes excluded from the traditional GBV sector (Calton et al., 2016; Strohmayer et al., 2019).

As we are promoting advocates as experts in their field, we wanted to give advocates the chance to be identified by their name and organisation should they choose to do so. As Reyes Cruz (2008) notes in her critical ethnography, academic discursive practices typically separate "literature reviews" from "findings" in a way that demarcates academic scholars (particularly influential dead white men such as Hobbes, Rousseau, Foucault, etc) as worthy of citing while

research participants (who are often from marginalised groups) are rarely considered worth citing as part of one's intellectual grounding. While participant anonymity may be motivated by good intentions like maintaining privacy, it can have the unfortunate effect of erasing or even appropriating participants ideas. Reyes Cruz (2008) asks instead, "Why don't I just cite Graciela?" (a woman who became an actor in her ethnographic work.) Consequently, although participants in the study are pseudonymous by default, participants could also opt-in to use their real name. Asterisks (*) indicate areas where participants chose to use a pseudonym or keep details confidential. This approach attempts to give participants more choice and agency in navigating the trade-off between privacy and attribution for their contribution. Participant names and organisations are listed in Appendix 1.

Participants were recruited using purposive sampling: some were recruited through my personal network, while others volunteered after the call was shared on a variety of mailing lists aimed at people in the victim support sector (see Appendix 3 for recruitment call). Selection criteria were having supported at least three survivors of technology-facilitated abuse. Interviews were recorded and transcribed using Word Transcribe, and then played back and corrected. Interviews took place over three months from December 2020 to February 2021 and were not compensated.

We asked participants about types of technology abuse they had seen, how they supported survivors, and what improvements they would like to see in technology and cybersecurity. Participants were also prompted to share specific cases, without identifying details, to illustrate how they supported different survivors. We also asked about how participants addressed the psychological distress which survivors experienced as a result of tech abuse, as well as whether there were any demographic factors (like gender, race or immigration status) particular to the survivors they supported that shaped their experience of tech abuse (see Appendix 2 for the full interview protocol).

Data analysis

Following the interviews, we hosted a two-hour long workshop to discuss the role of technology-mediated abuse in the development life cycle of data-intensive technologies[21]. Ten interviewees were invited back to this workshop, although only seven were able to attend. As part of this workshop, we carried out a 'data walkthrough' where we presented our initial data analysis back to participants, asking them to critique our interpretations. We used an

[21] The workshop results are described further here: https://nrl.northumbria.ac.uk/id/eprint/47508/

interactive whiteboard to support the discussions in the virtual workshop. This allowed participants to add their thoughts and reactions without words. We presented some initial findings from the interviews on the whiteboard, giving participants an opportunity to respond and push back on our interpretations verbally, as well as with post-it notes, emoji, or other forms of visual media on the whiteboard (see Figure 3). This process of participatory data interpretation allowed us to conduct research in a less hierarchical way, following feminist principles of participatory research (Gatenby & Humphries, 2000). We highlighted in the transcript and our findings moments when participants pushed back or re-framed some of our interpretation. The workshop was audio recorded and transcribed; we took screenshots of the whiteboard.

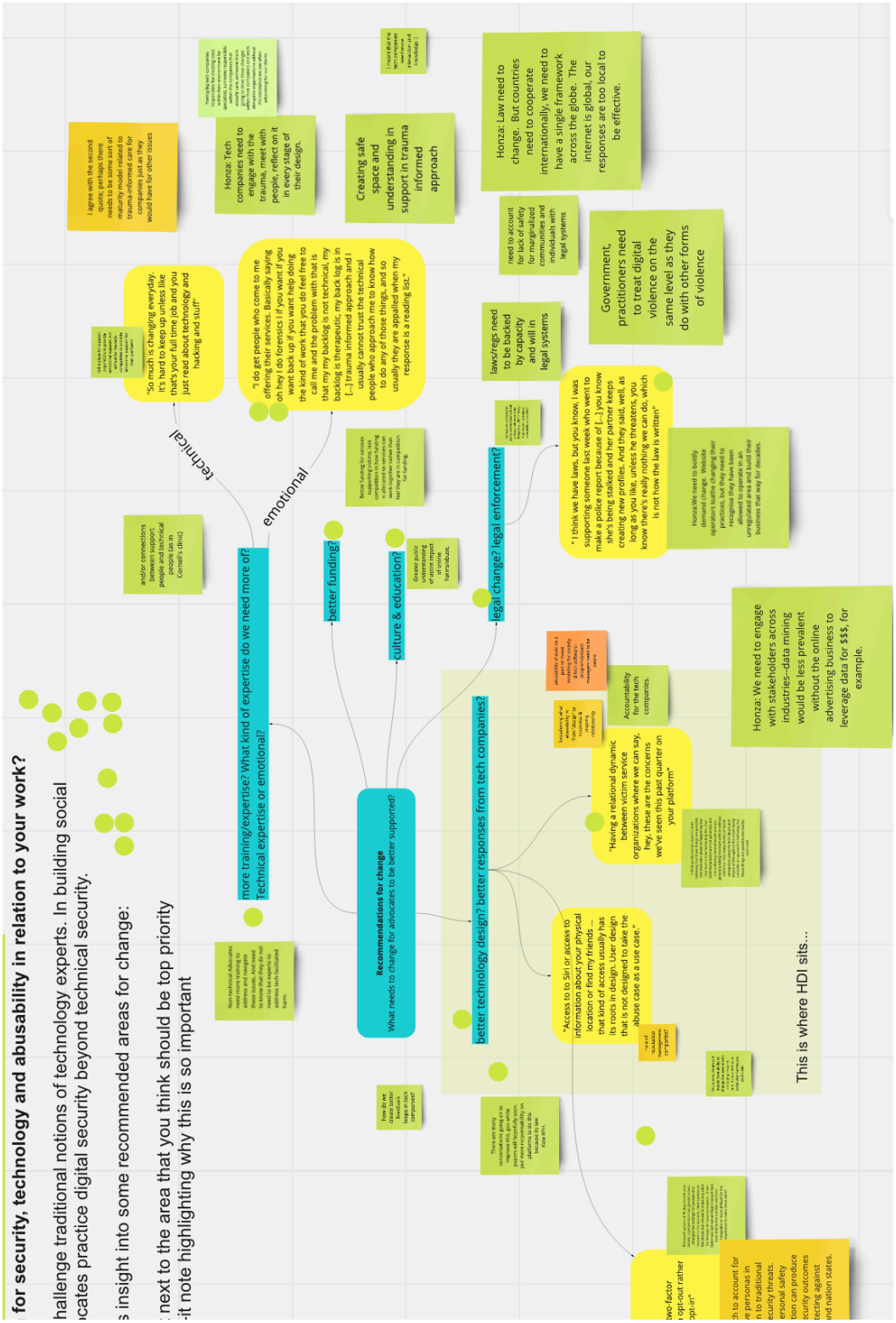

Figure 8: screenshot from data walkthrough workshop

The interview and workshop transcripts were analysed using reflexive thematic analysis (Braun et al., 2019; Braun & Clarke, 2020). This approach to qualitative analysis emphasizes the active

role of the researcher in the knowledge production process and intentionally does not include a codebook or quantification of frequency of themes. Instead, this work focuses on the reflexive development of understanding with and through the data: initially the first author coded the interview transcripts, from which they developed themes. These themes, alongside quotations from the transcripts, were fed back on by participants during the workshop. The transcript from the workshop was then coded and discussed by both authors. As such, the final themes presented in this chapter were negotiated between both authors, in conversation with participants, and based on data and our interpretations thereof (Braun & Clarke, 2020).

In September 2021 the authors worked together to produce a toolkit to improve the safety of people for technology developers and researchers who work closely with data-intensive technologies. This writing process helped crystalise themes and helped further develop our thinking. This learning also feeds into this chapter.

Ethics

This study received ethical approval from the University of Oxford Central University Research Ethics Committee. We obtained informed consent from participants to conduct and (optionally) to audio record the interview. As the interviews could touch on sensitive topics, we ensured that participants knew that they could skip questions and request a break at any time. We also emphasized that participants should provide only as much detail in their answers as they felt comfortable with. All electronic files were password protected and stored in a secure location.

Positionality

Both authors are white women feminist researchers in the United Kingdom whose research interests are related to safety and technology. The first author is a PhD student with some experience volunteering with a sexual abuse and rape crisis centre in their listening services, i.e., phone and texting support. This experience allowed for a degree of shared understanding and empathy with participants. The second author is safely employed at a university with experience of working with a number of support services who work with people of all genders who have experienced different forms of interpersonal, politically motivated, and institutional harms. The two authors bring their experience and gained understanding from their volunteering and collaborative research to frame the concerns outlined in this chapter. As such, our feminist approach, the centring of our collaborators' knowledge, and our somewhat-insider knowledge plays a crucial role in our analysis of the data.

Findings

In this section we address three main areas: (1) advocates' support practices; (2) the networked and relational forms of security that are produced in this process; and (3) the changes that these advocates propose in how we address tech abuse.

Support practices

Advocates described supporting survivors in five main ways: by establishing trust and belief; safety planning (which includes threat assessment, resilience mapping, and acting to secure accounts and devices); empowerment and demystification; supporting evidence-collection and making referrals. While some of these support practices—like threat assessment or securing devices—resemble established cybersecurity practices, others—like demystification—are more nuanced emotional or psychological practices which fall outside of conventional security frameworks.

Establishing trust and belief. Many advocates described establishing trust and belief as a critical prerequisite to providing any support. In our interviews, many stressed the importance of establishing a relationship before any probing questions about the abuse or survivors' devices were asked. Many survivors will have experienced gaslighting, an abuse tactic in which a perpetrator tries to undermine a survivor's perception of their own sanity. This is then often compounded by disbelief from friends, family, or law enforcement (Henry et al., 2020). Natalie Dolci, (Technology-Enabled Coercive Control Initiative (Cuomo & Dolci, 2019)) said, "it's very easy for [...] female identified survivors or gender nonconforming survivors [...] to be treated like they're crazy." Consequently, belief and validation—i.e., making sure survivors felt that their concerns were affirmed and taken seriously—were critical principles for most advocates interviewed.

One advocate described doing this through sharing her own experiences of technology abuse to reassure survivors that they are not alone in their experience and "build rapport" with them (Stephanie*). Many others repeated the importance of reassuring survivors that they believed them, that their experiences and emotions were not uncommon, and that they were not to blame for what had happened. Sol*, an advocate who had a day job in white hat hacking, contrasted these practices of belief and validation with "a more anxiety causing ... tendency to talk about the worst-case scenario and focus on that" among information security professionals. Practices like establishing trust, building rapport, and proactively communicating belief are important prerequisites to creating an emotional sense of safety, before beginning to assess

technical device security. This is important because without that trust, advocates might never be able to understand how they can support survivors.

Safety planning. A variety of practices including (1) threat assessment, (2) resilience mapping, and (3) digital self-defence--grouped under the term "safety planning" form a major part of the support advocates offer survivors. One way of understanding this is that safety planning is the most obvious substantive form of support, while the other practices outlined in this section are more subtle underlying practices intertwined with safety planning.

Firstly, after establishing trust, advocates often described conducting a formal or informal threat assessment (although most advocates did not describe this in terms of threat assessment). Assessing threats can include technical support like checking devices and accounts, but it can also be assessing for emotional, physical, or financial threats. Chris described this as a "kind of triage, like what do we need to take care of?" Recognising technology abuse alongside other forms of coercive control can be a challenge; several advocates reported that many survivors do not realise that technology abuse is happening as "it's not always very obvious" (Amy Jacques). Advocates emphasized the importance of paying attention to children's accounts and devices in threat assessment, as these can easily be abused. In many situations, survivors may not identify an abusive situation as abusive.

For example, Emma Pickering (Refuge UK) described a situation in which a survivor reported intense harassment of around 100 emails a day, but the police were not taking the case very seriously. Emma went through "a checklist with [the survivor] and it turned out that actually the whole house was rigged with technology. She'd been with him since she's 15 and she thought it was very normal because of the way he behaved to have webcams in the bedroom, the bathroom; he had three home-built PCs for the children, the Xbox was rigged." In this case, the survivor was aware of the cameras but had not articulated this behaviour as abuse and therefore did not report it to the police.

Threat assessment practices can come into tension with the principles of belief and validation. For example, Sarah explained "we always want to make sure that we're believing people, but I think for people who may be new to [...] working with someone who's experiencing stalking behaviour, especially if that stalking includes tech-facilitated abuse that they may jump to like the zebra issue instead of just working with horses first." She explained this meant both survivors and advocates may assume stalking is related to "more advanced" forms of abuse like spyware or hacking, when, mundane acts like guessing or coercing a Facebook password are much more common forms of compromise.

Identifying what's possible requires a detailed knowledge of account compromises, such as the fact that if someone has access to an email password, they can likely use that to reset your Facebook password, but not vice versa (Rowan*). Therefore, threat assessment often requires both fairly sophisticated technical knowledge (i.e., differentiating between spyware or various password compromises) as well as the very subtle practices of belief and validation discussed earlier. Advocates take great care to avoid invalidating survivor's experience of abuse, even if their assessment of the problem is different to the survivor's.

Many advocates reported incorporating the framework of intersectionality into their safety planning practices. They confirmed that tech abuse, like other forms of abuse, disproportionately affects people experiencing multiple forms of oppression. For example, survivors with disabilities who rely on assistive technology like mobility aids or screen-readers are particularly vulnerable to that technology being withheld or exploited (Natalie Dolci). Migrant survivors face specific risks like perpetrators impersonating immigration officials online and threatening deportation or threatening to expose undocumented status online. Similarly, Metzli Mejia, (Los Angeles LGBT Center) described how LGBTQ+ survivors face additional risks of being outed online. Lastly, many advocates reported that law enforcement are often less likely to treat cases involving women of colour or those from less wealthy backgrounds seriously. When taking these overlapping identities into account in threat assessment, advocates incorporate intersectionality into their practices.

Secondly, in the data walkthrough, Toby Shulruff made an important point in noting that advocates do not just assess threats, but also help survivors map their strengths and resilience. Toby noted that there is a tendency, especially in legal systems, to portray survivors as "fragile and in need of saving" when in reality they are highly creative and resilient. By mapping these strengths, advocates help survivors keep in mind all the resources they have to draw on; this is a critical part of empowerment, a practice explored in the next section.

Lastly, safety planning involves acting to secure accounts and devices, as well as anticipating future scenarios and planning appropriate responses with the survivor. Safety planning was, in advocates' accounts, often closely linked with "survivor centric approaches" which means "deferring to what the survivor identifies as best outcome" (Sarah). For example, rather than pressuring survivors to leave, advocates reported changing their advice and safety planning to adjust to the survivors' preferences.

Besides securing accounts and devices, safety planning may include actions like limiting social media use, or dating app use, reporting perpetrator to social media platform, or forwarding emails from the perpetrator to a separate folder to limit time spent engaging. Many of these

resemble what Akiwowo (2020) describes as "digital self care." Farah Sattar (DCRYPTD) described these as general "digital self-defence" techniques.

Advocates were careful to highlight potential unintended consequences to survivors: for example, removing spyware might result in losing the evidence that it was there in the first place. The difficulties of evidence-collection will be explored further in the section below on "Supporting evidence collection." Furthermore, removing a tracking app from a survivor's phone may result in further violence and abuse from a controlling partner, rather than making them safer. Therefore, it is imperative to incorporate the survivor's experiences, needs, context, and preferences into any advice.

Demystification and empowerment. Throughout supporting survivors who experience tech abuse, advocates seek to empower survivors to recognise their strengths while simultaneously demystifying the disproportionate power perpetrators attempt to project. As Eva Galperin (Electronic Frontier Foundation) said, "for a lot of people, technical knowledge and you know computer security is essentially magic […] so it's very easy to use the appearance of that knowledge to make yourself seem omniscient and omnipotent and often that alone is enough to manipulate the victim." Similarly, Chris said "a lot of times the abuser is promoting themselves as this tech god and they create an impression of themselves as just being all knowing and they can do anything." This overstating of perpetrator capabilities complicates threat assessment, contributing to the zebra vs horse problem described above. Advocates will demystify this appearance of power by helping survivors understand "what the perpetrator is actually capable of, and what's bullshit" (Eva Galperin).

Drawing on research from the Technology-Enabled Coercive Control Initiative (Cuomo & Dolci, 2019), Natalie Dolci phrased this in terms of "perceived expert status": perpetrators will often overstate their "tech-savviness" and advocates try to diminish this perceived expert status while raising survivors' perceptions of their own expertise and technical competence. Victim advocates have an informal mantra: *survivors have the most expertise about their own abuse* (Slupska & Lindsay Brown, 2021). Advocates try to deliver security advice in a way that respects survivor's expertise and allows them to make better informed choices rather than dictating their choices.

Advocates will both help survivors develop their technical skills and recognise how many technical skills they already have, in a process of empowerment. For example, Adam Dodge described asking survivors if they "know how to reset a password, know what location tracking apps are and what they do, know what Wi-Fi is" and when they answered yes, saying "I would describe that a person who knows how to use all those things and knows what they are as

actually very tech savvy." Similarly, for many advocates even mundane processes of threat assessment were phrased in terms of empowerment: for example, describing how to distinguish between annoying adware and targeted attacks as helping people "to be more empowered" (Toby Shulruff).

Survivors experience feelings of helplessness and disempowerment because of tech abuse, which limit their liberty (Cuomo & Dolci, 2019; Stark & Hester, 2018). This makes it particularly critical that advocates' security practices are based on empowerment as well as belief and validation. The technical support and advice advocates give needs to be survivor-centric and respect survivors agency to avoid repeating patterns of coercion and control. By improving survivors' perceptions of their own technical expertise, while simultaneously reducing the perpetrators' *perceived expert status* (Cuomo & Dolci, 2019), advocates aim to create a sense of safety which is synonymous with empowerment.

Supporting evidence collection. Although most advocates we interviewed were not lawyers, guiding and supporting survivors through interactions with law enforcement and court systems was a huge part of the work advocates described. Documenting device compromise, abusive messages, or oppressive surveillance are critical for seeking redress through legal routes, such as reporting to law enforcement, getting a restraining order, or going to court.

Advocates supported using tools such as "stalking logs" which allow survivors to record unwanted contact and interactions with perpetrators (Stephanie*). Advocates also often mentioned screenshots as a critical tool for producing evidence. Two advocates also described recommending a specific app called Our Family Wizard which is sometimes prescribed in court orders for co-parenting. Both advocates said this app was for making it easy to print a log of all text messages, phone logs and emails to provide to a court (although other advocates also expressed reservations about the way courts mandate it).

However, collecting evidence can often be very tricky. Many advocates noted the difficulties of procuring a record from private platforms like Facebook or Snapchat. Rebecca* described a particularly frustrating pattern with non-consensual intimate images shared on Facebook: "if you don't screenshot them before they're taken down, then it's really difficult to get information from Facebook, like get evidence of it for court." Getting tech companies (usually based in the US) to respond to requests for evidence is often even harder in countries outside the Global North: Andrijana Radoicic Nedeljkovic, an advocate at Atina, a human trafficking and domestic violence shelter in Serbia, described a case where the state prosecutor had to wait thirteen months for a response from Facebook.

In addition, judges often do not know how to interpret technical data relating to forensics. Likewise, law enforcement often does not have the necessary skills to collect evidence and preserve evidence, so that skilled defence lawyers can make "technical legal arguments around [...] in relation to the chain of evidence" (Milcah*). With harassment using anonymous platforms or spoofed phone numbers, attribution and demonstrating authenticity is a challenge. Because it is hard to "get physical proof that it's happening", tech abuse often is not "taken as seriously by different systems" (Rowan*). Hera Hussein (Chayn) tied this to "a hysteria amongst the [criminal justice profession] around women submitting false cases." Ben Walker (Tech-Enabled Coercive Control Clinic), described being unable to help survivors by providing evidence in court as then "our clinics records could become public as a result of subpoenas."

Technical capacities for collecting evidence can also themselves be abused. Hera Hussein described a case where a woman was recorded for ten years in her home by her partner without her knowledge. Her partner was now using those ten years of security camera footage against her to fight a custody battle by selecting footage that suited his case and omitted evidence of his own behaviours. This points to the ways that video evidence is valued very highly and often not examined critically by court systems. In this case, part of the support Hera was able to offer was to help the survivor validate her experience of being secretly recorded as coercive control: "you start peeling the layers that society has, like you know, put on women's minds about compromise and understanding the other person and they start seeing the situation for what it is. I think that is a very heavily underappreciated service to support survivors' understanding."

Supporting evidence collection is critical in criminal and civil legal systems, in all countries in which we interviewed advocates. Evidence can also be very psychologically important in the context of gaslighting, so survivors can be reassured their experiences are valid. Therefore, evidence collection, although it is not immediately related to securing devices, is crucial for accomplishing a broader sense of safety and security.

Referrals. Lastly, advocates support survivors by connecting them with various specialists, resources, and other support services. As Susan Hickey (Harris Country Domestic Violence Coordinating Council) said "we're kind of like [...] a bridge to other resources." To be able to refer survivors to these services, advocates first need to build networks of people who can be trusted to support survivors. This practice of developing and maintaining networks of care will be explored further in the next section.

Networks of care

Networks of care are networks of practitioners willing and able to support survivors with specific needs. Developing and maintaining these networks is a critical security practice that advocates do to create more supportive and caring environments for survivors, and in many ways a prerequisite to the individual support practices described in the previous section. The following section first describes the key attributes of these networks, and then explores two particularly tricky relationships to maintain: namely, with law enforcement and tech companies.

Defining networks of care. Networks of care have three key attributes: namely, they involve elements of care, education, and relationships. Firstly, these networks' purpose is to create caring environments for survivors. This support is often not just about pragmatic advice but also about showing care. For example, several advocates mentioned making connections with very local contacts, such as "Geek Squad" tech support services at an electronics store, or a local car mechanic. Susan Hickey explained, "I really like when car companies will say yeah, sure I'll come, and I'll look at your car [...] Maybe they're not going to see everything. But I think it just provides a survivor that support that's so important to know that there are people that care." As survivors have often experienced isolation and cruelty from perpetrators, as well as indifference or ignorance from legal systems, building experiences of care is crucial.

Secondly, building links in the networks of care often involves educating various stakeholders to prevent those actors from invalidating survivors' experiences in ways that contribute to gaslighting. For example, Susan described wanting to make sure a counsellor was "aware of all the ways a person could [...] use technology to abuse them [...] so they're not [...] like oh lady, you're crazy." Similarly, Rebecca* mentioned, "if there were say like a IT expert who could go through their phone with them but was not trauma informed, I would be nervous to refer someone to that person without also being there." A particular risk for advocates coming from the digital privacy or cybersecurity space is "judging [survivors] very harshly, scaring them, giving them advice that is meant for protecting them from nation states or law enforcement rather than their [...] abusers level of technical skill" (Eva Galperin). Therefore, building these networks is more complicated than simply identifying local services; advocates must also ensure that other actors in their network will take a caring, trauma-informed approach.

Lastly, the work of developing networks of care is highly relational as they require building and maintaining relationships. The emotional labour that goes into developing these networks--for example, anticipating how an IT expert may invalidate a survivors' experience--is not commonly appreciated as a kind of security work.

Law enforcement. Advocates described a complicated relationship with law enforcement: they must rely on the police to conduct investigations and enforce protection orders, while simultaneously trying to mitigate the many ways legal systems fail to address cases of partner and family violence. Andrijana Radoicic Nedeljkovic (Atina) described the risk of law enforcement not treating tech abuse like "real violence" which can create a confusing situation of "double messaging" for survivors after advocates have encouraged them to identify their experiences as abuse. For this reason, for many advocates it is important not just to support survivors in articulating abuse, but also to educate law enforcement to be more receptive and understanding.

Although many advocates described the importance of maintaining close relationships with law enforcement to ensure perpetrators are prosecuted, many also emphasized that "the vast majority of survivors don't report to law enforcement, don't want to be involved in legal systems for a full variety of reasons, or they approach legal systems, and legal systems aren't able to [help them]" (Toby Shulruff). As a result, most advocates agreed that the main source of support for survivors should "stay with NGOs and community-based organizations" (Toby Shulruff). Law enforcement is often implicitly assumed to be a solution to coercive control and domestic violence, yet it is often a part of the problem. Advocates are therefore an alternative source of security to that practiced by courts and police.

Tech workers and tech companies. Another significant group that advocates described building relationships with were tech companies and tech workers. Advocates often described a serious gap in support and care from large tech companies. Many advocates had reached out to tech companies and reported a variety of frustrating experiences. One advocate said, "computer emergency response teams at companies do not want to tackle tech abuse." Several advocates noted that it is impossible to get any form of human customer service from large platforms like Facebook or Twitter, "these monolithic companies that have no telephone number or they have no email address" (Chris). Even in very serious stalking or abuse cases, survivors must navigate complicated forms and help pages without support. "The ability to reach a person would be a game changer" particularly if there were "customer service people who specialised in identifying and supporting survivors of intimate partner violence" (Natalie Dolci).

This gap in support is being filled by tech advocates, often in ways that creates burdens for their organisations. As one advocate said, "the tech companies' lax attitude to customer service is remedied by people in the advocate/charity space, without compensation." Luiza* described an (ongoing as of time of writing) situation in which Pornhub, without seeking or getting

permission, links to her organisations' Facebook page on its "Non-Consensual Content Policy" website, which results in thousands of people from all over the world reaching out for support with cases of image-based sexual abuse. The advocate spent an increasing amount of her time helping people navigate Pornhub and other platforms, like Facebook's, non-consensual content policies. She said "the thing that's really disheartening and upsetting, is that, you know, someone reaches out to me to support them. Like immediately [...] like I'm really going to be like [...] Okay let me just get Mark on the phone quickly and I'm like yo Zuckerberg [...] take this down quickly." This is challenging as it often takes weeks to get non-consensual content removed, and then when it is removed, there is no support for getting evidence to prove it e.g., in a court of law. As a result, she said "It's like I don't have the funding anymore to do this work and I can't stop either right? [my supervisor suggested] it's an emotional strain to support people, right? And it's not like- this isn't my role [..] I'm not a trained counsellor."

In the data walkthrough workshop, we suggested that companies like Facebook or Pornhub should be providing more support to survivors, as it seemed the advocate in the situation above was doing unfunded customer support for these companies. Interestingly, this was partially challenged by Kate Worthington, a practitioner working with the Revenge Porn Helpline, who said, "I don't think I would trust the tech companies to take on that emotional support." She highlighted the importance of having support from independent organisations, as customer support services inevitably have the company's interest, which often differ from survivors', in mind.

Similarly, Eva Galperin described experts in forensics reaching out and offering to help her with the work she does supporting survivors, and said "the problem with that is that my backlog is not technical, my backlog is therapeutic, my backlog is in [...] trauma informed approach and I usually cannot trust the technical people who approach me to know how to do any of those things, and so usually they are appalled when my response is a reading list." This highlights the enduring importance of funding independent support services, alongside calling for better support from companies. Further recommendations for change will be explored in the next section.

Discussion

This chapter responds to the need we outlined in section 2 to study existing safety strategies to support victim-survivors of technology-facilitated abuse. In section 3, we present safety practices of individual advocates as well as how this work is situated in and promotes the

development of wider networks of care which incorporate different kinds of expertise - including that of people within the security sector.

To fully empower survivors, we would require a destruction of patriarchal social structures and the provision of adequate housing for survivors, social services support, and a variety of other support measures which are not new technologies. These are not issues that the security community can tackle on its own. However, there are ways in which the work that takes place within the community, especially that which aims to address the topic of technology-facilitated abuse and/or other forms of violence against marginalised people, can better support safety work. Therefore, we offer two key implications for the security community: (1) the need to redefine technical expertise; and (2) the need to recognize networked care work as central to security work.

Redefining technical expertise

As we outlined in Chapter 1, theorists in the framework of the ethics of care posit that experiences of caring for those who are vulnerable give care-providers access to distinctive insights on ethics. We follow and extend this tradition, showing how experiences of supporting survivors lead tech abuse advocates to develop valuable expertise on technology and digital security. Advocates in this space have developed a unique set of skills that combines technical knowledge with the emotional and therapeutic sensitivity needed to support people who have experienced trauma.

This finding departs from several existing studies of the tech abuse support ecosystem which highlight gaps in training and capacity in the sector, sometimes presenting support services as overwhelmed or ill-equipped to address the problem of technology abuse (Cuomo & Dolci, 2019; Tanczer et al., 2021b). For example, a recent study concluded that "both statutory and voluntary sector representatives 'don't want to be tech experts' [...] nor should they have to be" (Tanczer et al., 2021b). In fact, some advocates we interviewed also did not consider themselves to be "tech savvy."

This seeming inconsistency can be partially explained by our recruitment and well as through self-selection of participants. Unlike previous studies, we spoke only to advocates who were already interested in and knowledgeable about the problem of tech abuse (due to self-selection in response to the recruitment call). Their level of technology expertise is not necessarily representative of the broader community of practitioners in support services.

However, this tension is also linked to our desire to reframe what is commonly understood as technical expertise. Not every support worker in the field of domestic and sexual violence

should necessarily be viewed as a technology expert, yet each of them, including those who did not consider themselves tech savvy, will have valuable experience with understanding the dynamics of coercive control, as well as how technology can enable these dynamics.

For example, advocates consider intersecting systems of power and oppression, like misogyny, racism, or ableism, in their threat assessment; these factors should be considered in threat assessments more broadly. This offers a model of cybersecurity which is attuned to intersectional power relations. These findings resonate with findings from Chapter 2, which explore how community support networks help migrant domestic workers navigate interlocking systems of racism, misogyny, and xenophobic border controls.

Similarly, ideas such as focusing on the "horse issue" instead of the "zebra issue" are valuable for academic research and media reporting, which can fixate on flashy, sophisticated, but relatively rare, attacks like spyware and omit mundane and common attacks like coercing Facebook passwords. Advocates practices of belief, empowerment, and demystification, also point to the intertwined psychological, emotional, and technical aspects of information security.

Tech abuse advocates' expertise departs from conventional understandings of a "cybersecurity expert" which might involve someone with in-depth knowledge of cryptography or malware analysis. However, this expertise is incredibly valuable for understanding online safety and security. This expertise should be recognised by technology designers and companies looking to build safer digital systems. Many of these organisations also need to receive much more funding from government institutions to continue doing the important work that they do. We support calls for greater funding and training to extend the capabilities in the victim support sector, however we also want to highlight that this grounded knowledge translated into many valuable insights which the digital privacy and security community can learn from.

To integrate this new understanding of technical expertise, those developing and deploying technical systems should seek out and, crucially, compensate advocates who have direct experience with the harms their products can cause. Practitioners who work on the ground with people directly affected by the problem are a critical source of security expertise. This is true not just for the problems of technology-enabled coercive control or intimate partner violence, but also more broadly for other forms of abuse or discrimination that are exacerbated by technology, such as racism or xenophobia.

Likewise, security and privacy researchers should collaborate with such practitioners by employing participatory research methods such as those applied by tech abuse clinics (Cuomo & Dolci, 2019; Havron et al., 2019) or in "participatory threat modelling"(Slupska et al., 2021). Methods such as the ones I developed in Chapters 2-3 are pragmatic ways for security

practitioners to incorporate the expertise of advocates and support workers. Threat modelling both in research and in industry practices should include interpersonal harms such as coercive control, bullying, or stalking (Freed et al., 2018; PenzeyMoog, 2021; Slupska & Tanczer, n.d.). Incorporating the perspectives of both survivors of violence and practitioners who support them will help address blind spots in threat modelling and develop more robust security practices.

Networked care as central to security

Advocates work to create safety for survivors through empowerment, validation, and creating networks of caring, supportive people that survivors can rely on for support. Many of their practices (like threat assessment and safety planning) do resemble conventional security practices. However, practices like advocating for digital self-care or empowerment through technical skills clearly relate to digital security, yet extend far beyond ensuring technical security of accounts and devices. Many of these security practices resembled the tech support we offered at Reconfigure workshops (described in Chapter 3). These kinds of care work more closely resemble what Hörschelmann et al. (2016) describe as "webs of (in)security" or security practices which include the emotional and practical labour invested in dealing with the breakdown of social relations. It remains an open question whether it is more helpful to reconceptualise (some) care practices as security practices or move away from the notion of security entirely. In fact, advocates themselves rarely used the word "security", often speaking of "empowerment" instead.

This is reminiscent of critical security theorists' preference for emancipation or liberation over security. Critical security theorists emphasize that some security practices can be harmful, as when practitioners in the security industry will inflate threats to sell security as a product (Neocleous 2003). This form of tech saviourism can be disempowering or even exploitative to security subjects, exposing them to surveillance in the name of security, or leaving them in a permanent state of fear. Advocates supporting survivors are not in a financial relationship with survivors and do not need to sell them security products (as security practitioners in a company may be). Crucially, through their focus on empowering survivors and demystifying abusers' abilities, tech abuse advocates invest a significant amount of time and energy to reduce perpetrators' perceived expertise. This runs counter to many security practices of threat inflation which are critiqued within critical security studies.

Tseng et al. (2021) have noted that the language of "empowerment" can be misleading in this context, arguing that tech abuse support practices are better described as enablement, or the facilitation of "opportunities for people to develop their own capacity." As Erete et al. (2017)

write, technology interventions alone cannot empower people without addressing underlying social, economics, and political inequities. Survivors are often targeted because they belong to a systematically marginalized group and abusers know they can wield power against them. To describe projects and technologies as empowering when they do not truly shift these underlying power structures can obscure this reality (Tseng 2021). Although we cannot evaluate to what extent these practices are actually empowering, the fact that these advocates actively aim for agency and empowerment as a part of security is still significant, as it runs counter to many descriptions of security practices within critical security studies.

Privacy and security researchers and practitioners can draw several insights from the findings and questions raised in this chapter. Firstly, by learning about digital security practices in a very different context from the standard security setting (i.e., within a corporate or military organisation) security practitioners can reflect on their own security practices: for example, advocates actively incorporate the values of empowerment in their practices. What kind of values do security practices in other contexts incorporate? Collectively, the three studies in this thesis present community and care-based forms of security as a potential positive alternative to carceral state or corporate security.

Secondly, this study highlights the benefits of studying existing practices rather than prioritising the development of new technical solutions, offering a pragmatic alternative to technical solutionism. Having an awareness of security as a set of practices opens up the possibility of understanding the networks through which these practices take place. Practices such as developing networks of care in communities are a critical source of support for survivors of abuse and easily missed if the focus is solely on securing devices. Such practices have similarities to feminist work in addressing gender-based violence through developing safe(r) spaces discussed in Chapter 2. The possible points of intervention, therefore, are not only device design, individual change, or interpersonal relationships, but also the broader community and social environment. Computer scientists, although they may consider only device and systems design to be relevant to their work, are a part of these broader communities and environments. By thinking at the level of community and considering how to support this work of creating safe(r) spaces both on- and offline, we can develop a more feminist form of cybersecurity, or perhaps solidarity.

Limitations and directions for future work

In looking closely at advocates' support practices and exploring their understandings of security, we have accepted a variety of limitations which would have enriched our work and are important to explore in further research.

First, we focused our research design on interviews with advocates, not survivors (with a few exceptions where advocates had themselves experienced technology abuse) so we did not assess survivors' perspectives on these support systems. Therefore, we were only able to describe support practices as they were related to us by advocates; as with any practice, there is likely a gap between what practitioners describe and how this works in practice. This means we are also not in a good position to evaluate the "dark sides of care", i.e., how a care relationship can place a care-giver and care-recipient in an unequal power dynamic. Methods such as ethnography and participatory observation, as well as interviewing survivors about their experiences, would provide a richer picture. Survivors' experiences of abuse have been a significant focus of research (Matthews 2017, Freed 2017), but their experience of support practices and their ideas about safety would undoubtedly be very valuable for future work.

More broadly, we do not fully engage here with existing debates on accessibility and inclusiveness within the field of coercive control and gender-based violence. For example, because of the severe isolation that often comes with abuse, many survivors are not able to access support services in the first place, while others have reported negative or exclusionary experiences at support services (Sokoloff & Dupont, 2005). Scholars and practitioners advocating for abolitionist perspectives warn that close relationships between intimate partner violence services and law enforcement are a barrier to access for marginalised groups who are disproportionately targeted (Cuomo & Dolci, 2019; Sokoloff & Dupont, 2005). Additionally, others are concerned that a sector originally developed to support "battered women" does not adequately support male, LGBTQ+, trans or non-binary survivors of abuse (Calton et al., 2016; Faye, 2021; Guadalupe-Diaz & Jasinski, 2016; Powney & Graham-Kevan, 2019). These issues are contested and complex, and they warrant further study to see how they intersect with privacy and security concerns.

Conclusion

Advocates who support victim-survivors of technology-facilitated abuse provide cybersecurity support and develop cybersecurity expertise through their work, making them (often un-acknowledged) cybersecurity workers and experts. Through their work in developing safety strategies and the sustainable establishment of networks of care, these advocates reconfigure cybersecurity as a form of care sensitive to the experience of trauma as well as broader structures of oppression and discrimination. With this chapter, we expand the security and privacy community's understanding of this kind of work, and how it can be adapted into security research practices. We do this by (1) expanding the field's understanding of what

'technical' support in security studies is and could be, adding layers of care and relational support; (2) questioning conventional understandings of security by adding the notion of care work as integral to the work of security experts; and (3) redefining technical expertise in security, including knowledge from experiences of support workers and advocates. To better support victim-survivors of technology-mediated abuse, we argue that the security community must re-evaluate its understanding of technical expertise to validate and incorporate the expertise of advocates and recognize the individual and networked care that is inherent to this work. Once we recognise and understand these networks of care, we can build on and extend them though expanding threat modelling to account for harms like coercive control and structural forms of discrimination (Chapter 3) and employing participatory methods (Chapter 4). Collectively, these three studies present community and care-based forms of security as a potential alternative to carceral state or corporate security.

Acknowledgments

Many thanks to our participants, without whose ideas and dedication this work would not be possible. Thank you also to Helena Webb and Gina Neff for invaluable supervision and support. Parts of this work were funded by the EPSRC EP/R045178/1 Human Data Interaction: Legibility, Agency, Negotiability' and the EPSRC Studentship as a part of the Oxford Centre for Doctoral Training in Cybersecurity.

Chapter 6: Abusability[22]

Chapter summary

In this chapter, I explore how cybersecurity can account for the abusability of systems. Abusability, which plays on the concept of usability to ask what kinds of uses should be restricted rather than enabled in design, is defined as a quality that assesses how easy it would be for malicious actors to hijack or weaponize a system for harmful activity. I start with an overview of design recommendations from the tech abuse advocates interviewed in Chapter 5. Building on their recommendations, I expand on the concept of abusability with a discussion of how design practitioners can incorporate the threat modelling method outlined in Chapter 3. By considering power dynamics, incorporating safety concerns into design and testing, and collaborating with support practitioners to build responsive systems, both security researchers and practitioners can reconfigure cybersecurity practices to centre people's safety in technology design. I then reflect on the opportunities and limitations that techniques like threat modelling and abusability offer to the broader problem of tech abuse. Although it can be strategic for advocates to learn and deploy the language of technology design, such concepts can assume responsible behaviour from technology producers and miss the underlying political economy in which these products are made.

Introduction

When developing new technologies, designers like to focus on the positive: what will this enable? What will this optimise? How will it change the world (for the better!)? As a discipline, information security often handles the negative, asking instead, how can something go wrong?

---

[22] Author statement: this chapter was written based on a toolkit titled "Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions", co-authored with Angelika Strohmayer, Julia Slupska, Rosie Bellini, Linda Coventry, Tara Hairston, and Adam Dodge as well as a paper titled "Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety" co-authored with Angelika Strohmayer and Rosie Bellini. Although Dr Strohmayer led on overall project coordination, the sections of the toolkit and paper used in this chapter (except for the section used as a quote) were solely authored by me. I also helped organised the data walkthrough workshop and conducted and analysed the interviews which inform the chapter as well as the toolkit. For this chapter, I combined sections of the toolkit and paper and expanded further with a case study and section on paradoxes.

Yet the way infosec experts ask these questions is usually too narrow, focusing on how an external malicious actor might penetrate a system to steal data or wreak havoc, rather than how an authorised user might (mis)use the system for harm. Likewise, designers often assume authorised users are not malicious. This section explores the concept of 'abusability', which offers a potential route to more systematic and rigorous methods for mitigating abuse of technology.

Abusability is defined as a quality that assesses how easy it would be for a malicious actor to hijack or weaponize a system for harmful activity; designers have a responsibility to anticipate and mitigate this (Calderon et al., 2019). In this sense, abusability is like the concept of 'dual use scenarios' in cybersecurity and weapons research. Many technologies, like nuclear power or artificial intelligence, can be used for both military and peaceful purposes. The challenge of diplomacy on dual use technologies is to allow innovation while limiting harmful uses. Abusability addresses similar problems at the level of interpersonal, rather than international, relations.[23] The concept of "abusability" plays on the concept of "usability" to ask what kinds of uses should be restricted rather than enabled in design (Greenberg, 2019.) In doing so, it invites designers to anticipate, mitigate and respond to abuse in the same way that designers might consider usability at various stages of the product development lifecycle.

This concept extends and operationalises my conceptual reconfiguring in Chapter 2, as well as the empirical findings of Chapters 3-5. In particular, this chapter draws on the interviews with advocates in Chapter 5 as well as two workshops with advocates and academics. It also incorporates work from research from a toolkit on safety in human-data interaction which explores how abusability can be incorporated in the product design lifecycle (Strohmayer et al., 2021) and a paper on moving from "security" to "safety" in design (Strohmayer et al., 2022). Lastly, I explore two paradoxes in the concept and practice of abusability. These studies help me answer the ORQ: "*How can we reconfigure cybersecurity practices to account for technology-enabled coercive control?*"

Although other chapters discuss cybersecurity practices like threat assessment or problem definition, cybersecurity design practices (including threat modelling) make a huge part of the field. Therefore, this chapter returns to design practices, which I argue can account for tech abuse in three ways. First, designers and security researchers must understand that harm can

[23] Although in this chapter I primarily discuss abusability in the context of interpersonal relations, it can also be extended to systemic issues like police or immigration enforcement's abuses of surveillance technology.

come from the user or consumer: this requires abandoning a "customer is always right" mindset and considering power dynamics in technology use. Second, designers and security researchers should partner with experts (both practitioners and survivors with the expertise of lived experience) on abuse (such as intimate partner violence, sexual violence, racist abuse, etc.) to develop responsive systems. Last, designers and security researcher should approach abusability with the mindset of *responding* to rather than *solving* abuse: by accepting that abuse will occur and focusing on minimising the potential for harm and redressing harms rather than *erasing* them, we can develop a mindset of ongoing responsibility rather than technical solutionism.

The contributions of this chapter are primarily pragmatic—i.e., recommendations for altering threat modelling & building more responsive systems for design. However, I also develop the concept of abusability and outline how it contributes to my reconfigured understanding of cybersecurity. These advances are a result of my conceptual framework, which opens up a new way of understanding cybersecurity.

Advocates' recommendations for change

At the end of my interviews with advocates who support survivors of technology abuse (described in detail in Chapter 5), I asked "What problems have you identified in the design of digital technologies?", and sometimes as a follow up prompt, "What would you want to say to companies that produce and sell these technologies?" Advocates also made a variety of recommendations for how to address the problem of technology-facilitated abuse. These recommendations are important because, as advocates are not widely recognised as tech experts, their ideas for how to improve technology safety usually have not been included in privacy and security discussions.

Many of their design recommendations related to higher levels of privacy and security by default, such as setting a notification reminder to periodically prompt deletion of location data (Ben Walker) or sending notifications when someone logs into your account from a new device. Others made recommendations related to content uploads and moderation. Companies are often incentivised to coax users to upload as much engaging content as possible at the cost of safety. Advocates called instead for practices which prioritised consent and mechanisms for removing harmful content over data collection and engagement. For example, one advocate suggested, "the upload button on websites needs to be the same size/prominence as the report button" (data walkthrough). Others emphasized the importance of having these reports read "at the same quick speed it is to upload the content" (data walkthrough). Andrijana Radoicic

Nedeljkovic suggested that platforms could use facial recognition to notify people when someone uploads a photo of them, and to "be sure that the person had given consent."

Mechanisms for reporting could also be much more trauma-informed. For example, when reporting on forms and websites, survivors often are not informed about outcomes, so "you don't get that validation. You know it's all just like, well, you've made this report allegation thing, and we'll kind of have our own really opaque internal process about what's going to happen. So that is not very survivor friendly or validating" (Toby Shulruff). By understanding what good support practices look like (outlined in Chapter 5), companies can create better support mechanisms for survivors. In many cases, building better systems for care will be more important than designing better products or features.

Many recommendations for technology design related to broader processes and practices at tech companies rather than specific UX changes. Advocates showed awareness that product design related to the design process, saying "access to information about your physical location through Find My Friends [...] usually has its roots in design. User design that is not designed to take the abuse case as a use case." Advocates suggested incorporating tech abuse into conventional security practices like threat modelling or maturity models, saying "perhaps there needs to be some sort of maturity model related to trauma-informed care for companies just as they would have for other issues."

Natalie Dolci called for "a relational dynamic between victim service organizations where we can say, hey, these are the concerns we've seen this past quarter on your platform." This would allow victim service organisations to flag problems as they arise. Drawing on the concept of networks of care introduced in the previous chapter, this would mean tech companies would value and become embedded in these networks, rather than promoting themselves as the sole "solvers" of social problems. This was contrasted with disregard or tokenistic inclusion by companies, in which survivors or advocates were only asked for "green stamp" approval on solutions which had already been developed.

Case study: Facebook's intimate image hashing

One such case can be illustrated by the case study of intimate image hashing first proposed by Facebook. In 2017, Facebook revealed an unconventional plan to respond to cases of non-consensual image sharing on the platform. Facebook invited people who were concerned about their intimate images being posted on Facebook non consensually to upload the photos they were worried about to Facebook. Facebook would then 'hash' the photos, saving the hash but not the original photo, and then block that photo from being uploaded if someone

tries to upload them to Facebook, Instagram or Messenger. A hash is a numerical representation of a file, which allows Facebook to detect uploads of that file without storing the original data. The use of this novel and unfamiliar technology to combat abuse gained a lot of media attention, with headlines like "Facebook wants your nudes to tackle revenge porn" (Cafolla, 2017; Cao, 2017; Limer, 2017; Statt, 2018).

Some commentators responded positively, noting the benefits of this policy: it aimed to prevent abuse (rather than merely taking images down once they were uploaded) and it enabled victim-survivors to report an image only once, stopping them from having to launch new reports each time an image was uploaded. It also included repercussions for posters, such as account deactivation (E. Smith, 2017).

However, the Facebook hashing pilot was also had several critical flaws. Firstly, the solution assumed users have access to the image they are worried about being shared; in many cases, survivors of abuse have images taken of them without their consent or even knowledge, which means they may not have access to the image. Secondly and perhaps more importantly, the solution relied on survivors and advocates to understand hashing and trust Facebook enough to share sensitive photos. It was striking how the hashing solution relied on a survivors of intimate image abuse sharing their intimate images even further with a large corporation: an act that could easily be retraumatising. As one of the advocates I interviewed, who was directly involved with the pilot, shared, "that pilot really relied heavily on number one that the person trusted the system, trusted Facebook and [number two] that the staff person at our Association had the language and the support to walk someone through the process [...] I it's not my role to have people trust Facebook. That's not in my wheelhouse, yeah?" In practice, advocates struggled to explain the feature and did not see it as their role to get people to trust Facebook. It's not clear how many, if any intimate photo uploads where successfully blocked because of the feature.

Advocates were brought into the process after the solution—hashing—had already been selected by Facebook's safety team. The use of a complex and relatively unfamiliar technology like hashing, although helpful in generating media attention for the solution, escalated the problem that advocates had in understanding and explaining the policy to the survivors it was meant to help. In this sense, the Facebook hashing pilot includes an element of flashy tech-solutionism. Consulting advocates before the design and development stage rather than after implementation is critical for meaningful engagement. Furthermore, this case study illustrates a dynamic in which tech companies conflate "trust" and "trustworthiness",

investing resources in getting consumers to "trust" their product rather than creating a system which can truly be trusted to address abuse (Bellini in Strohmayer et al., 2021). In this case, the company tried to involve advocates in the process of increasing survivor's trust in the product, rather than involving advocates from the start to increase the actual trustworthiness of the product.

In December 2021, Facebook renewed the hashing initiative in a new form: the "Stop NCII" project run by the Revenge Porn Helpline, in partnership with over 50 other non-government organisations (Davis, 2021). I did not interview anyone involved with this new iteration, however its implementation would be an interesting area for further study, to evaluate to what extent this solution addresses the issues identified in the first one.

Participants in the study emphasized that more support and funding for training in building capacity is needed. This echoes a general concern with insufficient funding and resources in the field (Cuomo & Dolci, 2019; Tanczer et al., 2021). Some argued it would be more sustainable to develop more partnerships and collaboration with digital security practitioners. This applies also to the digital privacy and rights space: advocates noted that many online privacy resources are directed at politicians, activists and journalists and not intimate partner violence survivors.

Lastly, Luiza* called for more company measures aimed at perpetrators rather than survivors: "all these platforms can target advertising at a particular person [...] they know that I like ice cream and I'm in the neighbourhood and boom, there's a coupon that's going to come directly to me on a hot summer day. [...] why can't they use the same resources and tools to direct public awareness messaging at perpetrators?" This echoes calls in the literature like Bellini et al., (2020) to shift the responsibility for addressing tech abuse from survivors to perpetrators.

Advocates' recommendations for addressing tech abuse included more funding and resources for capacity building in law enforcement and the support sector, product design in which safety and security are built in by default, and better responsiveness when advocates and survivors raise problems. These recommendations are grounded in an understanding of security as networked and relational: to adequately respond to the evolving problem of tech abuse, tech companies and security workers need to develop respectful relationships with advocates working on these problems on the ground.

Abusability in product design lifecycles

As I outlined in Chapter 3, conventional information security places an intense focus on how an external, malicious actor (or actors) may penetrate a system for sabotage or financial gain, over examining the complex privacy and security practices inherent to social relationships. The concept of 'abusability' offers a way expand the focus of traditional approaches to security: abusability plays on the concept of usability to ask what kinds of uses should be restricted rather than enabled in design.

The following section develops three implications for incorporating abusability at various stages of the product development lifecycle:

Consider power dynamics. Rather than depicting users of a system as interchangeable and well-meaning actors, designers must consider the inherent power dynamics in societies structured by gender, race, ability, age, and other hierarchies of difference (Collins, 1990; Constanza-Chock, 2020). For example, as I discussed in Chapter 3, smart home devices such as locks or cameras which have different account types for "Owners" and "Guests" create a hierarchy of affordances which can reinforce abusive dynamics in the context of family violence or coercive control. Although such hierarchies might be useful or desirable for many users or potential consumers, designers should consider the implications of implementing hierarchy into design, and endeavour to make such hierarchies clear and understandable to all users of a potential device or system. This must also include consideration of broader, structural power dynamics: for example, as proposed by Sim & Zevenbergen (2017), designers of systems looking to address gender-based violence should be cautious of defaults that connect the user to law enforcement. Abusability is a reminder that power will often be abused, or as the old feminist slogan puts it "abuse of power comes as no surprise." Police are perpetrators of technology-enabled abuse, both in cases of police-perpetrated domestic violence and in their everyday policing practices (Centre for Women's Justice, 2020; No Tech for Tyrants, 2022).

Include safety concerns in threat modelling and testing. One practical way designers can incorporate abusability is by reconfiguring design practices such as threat modelling and usability testing to include interpersonal harms such coercive control, bullying, or stalking. Threat modelling both in research and in industry practices should ask "how might this product be abused for harm?" to allow for safety by design (PenzeyMoog, 2021). Chapter 3 offers an illustration of how designers can do this in the specific case of smart home devices. By drawing on existing social science and human-computer interaction (HCI) research on interpersonal abuse, researchers can develop threat models that can be used in industry product development. This is true not just for the problems related to coercive control or intimate partner violence, but also more broadly for other forms of abuse or discrimination that are

exacerbated by technology, such as racism or xenophobia. Further research on new forms of technology-enabled abuse, as well as forms of abuse that have received less attention (such as abuse of marginalised groups like migrants or domestic workers, or intersectional abuse that combines racism and sexism or other forms of discrimination) is also critical. Researchers and practitioners conducting usability testing can also develop abusability tests that include abuse scenarios akin to penetration testing, in which a malicious actor attempts to use the product for harm (see e.g., Parkin et al., 2019). Results from such tests should be fed back into product documentation or policies, or in more serious cases, researcher and practitioners should advocate for 'refusal' (Gangadharan, 2019): products with a high likelihood for abusability should be withdrawn or sent back for rethinking and redesigning.

We also need detailed data from companies on reported (or detected) cases of abuse, including disaggregated demographic data on gender, race, age, and other details. This would help researchers and policymakers understand broader dynamics of abuse. A contrast with conventional cybersecurity breaches is helpful here: in most jurisdictions, companies are now required by laws such as the General Protection Data Regulation (GDPR), to report breaches of consumer data. These reports in turn inform and validate threat models in security research. Data on reported abuse and harassment cases across various platforms would help researchers and technologists develop more robust abusability assessments and mitigations.

Develop responsive systems. Although abusability is critical at the design stage (where it is preventative), it is also important to address abuse once it has happened by developing responsive systems. At the most basic level, this entails including blocking and abuse reporting features on any platform or product which allows for interpersonal interaction. Abuse often occurs on platforms where it is unexpected, as is demonstrated by the case of abusers sending $1 bank transfers to send abusive messages[24]. Bank developers (understandably) did not consider a use case in which users may need to block others from sending them money; while this may have been flagged by incorporating abusability into threat modelling, it is also important to have prominent and accessible abuse reporting features so problems can be flagged as they arise. As Natalie Dolci suggested in Chapter 4, we need a *relational dynamic* between technologists and support services such as intimate partner violence shelters and sexual violence counselling, in which advocates are taken seriously and compensated fairly in

[24] https://www.sbs.com.au/news/people-are-using-1-australian-bank-transfers-to-send-someone-an-abusive-message/eab4d533-ac85-4f9f-8a6f-8cd71928070d

efforts to flag problems and develop support systems for those who have experienced technology-mediated abuse.

Such initiatives must also be careful of the pitfalls of *ethics-washing*, i.e., performative displays of interest in countering abuse without meaningful action and *tokenism,* i.e., seeking approval on an already developed project from advocates or survivors without meaningfully consulting them. For example, a rising criticism against technology companies has resulted in a spate of *Trust and Safety* or *Responsible Innovation* positions, but questions remain as to whether and when those teams have enough power to shift design decisions (Macgillivray & Wong, 2020). These risks are also illustrated by the Facebook intimate image hashing described in the previous section. As I expanded in Chapter 2, both researchers and practitioners can draw on the principles of participatory action research and co-design to ensure meaningful and respectful engagement with both survivors and advocates (Sim & Zevenbergen, 2017).

By considering power dynamics, incorporating safety concerns into design and testing, and building responsive systems, both security researchers and practitioners can reconfigure cybersecurity practices to centre people's safety in technology design. Cybersecurity concerns have fleshed out frameworks and industry standards for verification, monitoring, and certification, such as the US Department of Defence's Cybersecurity Maturity Model Certification (CMMC)[25]. There is ample work remaining to develop frameworks and industry standards for evaluating the abusability of existing systems and the extent to which developers account for abusability in design, but in our Trust and Abusability Toolkit, we start some of this work. We propose a basic rubric for evaluating the maturity of abusability practices (see table 1); this is a high-level overview and not a full maturity model that would be used in industry; however, such details should be fleshed out in the future.

Maturity level	Description
-2: Actively facilitating abuse[26]	Company designs and sells spyware or covert monitoring devices which actively enable abuse
-1: Wilful ignorance	Company either ignores the problem of technology abuse or addresses it superficially through:

[25] https://crest-approved.org/the-cybersecurity-maturity-model-certification-cmmc/index.html

[26] Thank you to Toby Shulruff at the National Network to End Domestic Violence for pointing out this lowest level.

	Ethics-washing: a performative display of interest in countering abuse without meaningful action **Tokenism:** seeking approval or a "green stamp" on an already developed project from advocates or survivors without meaningfully consulting them
0: Organisational awareness	Key decision-makers in company demonstrate an awareness of technology abuse broadly (through reading key resources) and how technology abuse occurs in their products and platforms specifically. This includes research and active reflection on questions like: What kinds of abuse occur on our platforms, products, or devices? Who is disproportionately affected by this kind of abuse? How does this abuse relate to specific product features?
1: Taking action	Company has taken action to mitigate and redress abuse on its platform or using its products, for example through: - Including tech abuse in threat modelling or abusability testing - Understanding how measures implemented to prevent abuse-such as reporting features or content moderation-can themselves be abuse - Incorporating abuse into content moderation policies and features (such as automated detection) linked to abuse reporting function - Offering options to survivors such as blocking perpetrators
2: Meaningful engagement	Company actions to address abuse incorporate abusability using principles of "trauma-informed" or "coercive control resistant" design. Tech abuse survivors and advocates are consulted at different stages of product development, their input is fairly compensated, and their feedback is taken seriously (in contrast with level -1 where advocates are only consulted after product is developed).

Table 1: Abusability Maturity Model. Originally published in Strohmayer et al.'s Trust and Abusability Toolkit: https://nrl.northumbria.ac.uk/id/eprint/47508/

Paradoxes of abusability

Concepts like threat modelling and abusability are useful for tech abuse advocates and researchers to engage with and critique technology design. A quick review of the concept of

abusability shows that it is not merely a quality of a system, but also a normative claim: namely, that technology designers *should* consider how their products might be abused or facilitate abuse. It is important to hold companies responsible when their technology enables abuse, or when they fail to take action that could prevent harm. The past few years have seen an ongoing negotiation of responsibility in which the responsibility has increasingly shifted away from victims burdened with "safety work" and towards companies and lawmakers to build safer systems and prevent harm.

However, it is important also that these concepts are deployed critically and thoughtfully. In this final section, I discuss three potential paradoxes raised by the notion of abusability.

Firstly, I have argued throughout this thesis that technology innovations should not be seen as the "solution" to problems of abuse and coercive control. Therefore, it may be surprising in this chapter to focus on improvements in technology design. As we argued in a 'Trust and Abusability Toolkit' (Strohmayer et al., 2021):

> "We want to very strongly refute the thought that if only we are able to design the right kind of technology or the right kind of feature in our data-intensive systems that we are able to make people entirely safe. Rather, we would argue that this technology-centred approach to the abuse of data and data-intensive systems to perpetrate violence against individuals is in itself harmful."

If technology design does not solve social problems, why focus on technology at all? Technology will not solve the problems of abuse, but as technology mediates our social lives and can exacerbate existing problems, technology design is a necessary part of the response to abuse. As a part of thinking more broadly about safety rather than security, it is impossible to 'design out' all forms of harm in our digital systems and create perfectly safe systems (Strohmayer et al). However, in line with feminist thinking on safe(r) spaces, it is important to focus on how to build devices and platforms which are as safe as possible (rather than perfectly safe). Abusability accepts that, for the foreseeable future, interpersonal abuse using technology will happen. This allows for "conscious development and adaptation for *when* (rather than *if*) harm is caused by or through our platforms" (Strohmayer et al.) The focus is therefore on harm reduction and restitution for survivors.

Second, is it deterministic to assert that any given product or feature can be evaluated for its potential for harm? Technological determinism—a form of argument in which certain social behaviours are seen as inevitable products of technological innovations—has been routinely critiqued as reductionist within sociological theories of technology such as science and

technology studies (Mackenzie & Wajcman, 1999; Wyatt, 2008). Abusability may seem to imply that there is something inherently 'abusable' about certain features, when the ways users adopt and subvert technologies for their own ends are inevitably messy and contingent.

This was evident in the debates among migrant domestic workers about surveillance cameras in Chapter 4. Some MDWs saw cameras as a "weapon" which they could use to defend against false accusations by employers, while others saw the camera as a trap which led them to feeling watched constantly, and an obstacle to escaping abusive employment. Similarly, although advocates I spoke with in Chapter 3 often discussed how perpetrators used smart home or doorbell cameras to monitor survivors, at least one advocate enthusiastically praised doorbell cameras as enabling survivors' self defence.

Furthermore, as the discussion of mitigations in Section 2 of this chapter illustrates, features which are installed for the purpose of security can also be co-opted by abusers. For example, a register of login details which alerts a user to the location and timestamp of logins to an account can help a survivor realize if their account has been compromised. However, it can also aid a perpetrator in stalking or surveilling their target (Parkin et al., 2019). Features like password resets, which may help a victim-survivor take control of a compromised account, can also be used by an abuser to lock a victim-survivor out of their account.

This points to the ways the same device, feature or technology can be used in a myriad of different and opposing ends. Given these contingencies, does it make sense to speak of any given device as more or less "abusable"? In many of these cases, who is able to benefit from these surveillance technologies is strongly linked to who installs and controls them (Geeng & Roesner, 2019), which is in turn linked to gender and a variety of other power dynamics within the home (Kennedy et al., 2015; Leitão, 2019; Strengers et al., 2019). This suggests the best response is not a question of design, but of education or underlying gaps in wealth or skills.

The extent to which any one technology or design is more or less "abusable" than another may, to some extent be an empirical question. In fact, in an earlier version of this chapter, my co-author and I called for "detailed statistical data gathered by statutory and voluntary support organizations, academia and industry stakeholders" to support the validation of threat models. Certainly, more data around, for example, abuse reports on platforms like Facebook or Twitter, could help inform research on safety by design by pointing to increases in abuse related to specific features. Organisations like the UN and the Centre for Disease Control are also working on developing measures for online gender-based violence to improve the global evidence base on its prevalence across countries (Wilton Park, 2022). However, questions of abusability are also difficult to measure empirically. For one, it is ethically questionable to vary design types to

link specific design features to more or less abuse. Reports of abuse are also likely to reflect the design of abuse reporting features (Crawford & Gillespie, 2016); recall that one advocate in Chapter 3 suggested, the "flag abuse" button should be just as large as "report content."

Furthermore, we must recognise that what counts as abuse is itself shifting, contingent and socially constructed. The existence and adoption of certain technologies may normalize certain behaviours—such as tracking a friend or a loved one with GPS—which would have been creepier or controlling before the widespread availability of apps like 'Find My Friends.' Following theories of the social shaping of technology, technology is both shaped by and shapes society and social life.

The critical security focus on *security practices* which I have adopted in this thesis offers a way out of this puzzle. Similarly, to security, abusability should be seen less as an objective state which can be measured (so that any device is x% abusable), but rather a call for a set of practices: threat modelling, abusability testing, abuse reporting, which will create more responsive design systems. 'Design systems' here means processes (such as collecting and analysing data on abuse reports) and collaborations between actors both in industry, academia, and the support system which continue ongoing conversations on defining abuse, understanding how it can be perpetuated with technology, and developing responses to challenge it. Far from being a product of technological determinism, abusability can be a part of the social construction of technology, which recognizes that the path of innovation is shaped by society through culture, politics, economic arrangements, and regulatory mechanisms (Whittaker, 2021).

The final paradox in this call for abusability, which is arguably the most serious one, is that abusability presupposes a level of good will on behalf of platforms and other technology producers. It treats a lack of foresight on how products might be 'hijacked or weaponised' as an oversight. However, it does not necessarily consider how platform incentives may not align with mitigating abusability. In some cases, user safety may be seen as overlapping with profit incentives: after all, users may leave platforms or products where they do not feel safe. But in other cases, addressing concerns around safety and abuse is seen as an expenditure rather than a source of income (Macgillivray & Wong, 2020).

In the worst cases, however, selling abuse products is directly a part of the business model, as in the case of covert surveillance devices or spyware. What is the point in asking a spyware company to consider the abusability of their products when abuse is their business model? And spyware may be an unnecessarily extreme example: collecting granular and potentially sensitive user data usually creates opportunities for abuse, making platforms like Facebook into

a “stalker’s paradise”(Freed et al., 2018b). Yet this data collection is critical to almost all major platforms’ business models.

The past years have seen increasing prominence of “Trust and Safety” teams at major tech companies. Questions remain about whether these teams are sufficiently resourced, or have sufficient power over design decisions, to meaningfully implement the concept of abusability in the design process(Macgillivray & Wong, 2020). There is risk that these teams are a tool for ethics washing (as discussed in the maturity model in Section 3). However, pressure from external advocates have led to these teams being given more power. Therefore, it is valuable for tech abuse advocates and researchers to continue to critique business practices. Once these concepts and terminologies are made accessible to the IPV sector and refined to account for victims’/survivors’ concerns and needs, they will offer IPV researchers and practitioners a language to advocate for design changes and critique current industry practices. Furthermore, there is a value in developing alternatives to current design practices (i.e., showing how things *could* be different if abusability played a more prominent role in design), even if further work remains to outline how to get to those alternatives despite (or perhaps after dismantling) the current constraints of political economy.

Conclusion

In this chapter I introduced the concept of abusability and, drawing on my conceptual framework as well as insights from advocates who support survivors of abuse, offer three routes for incorporating abusability in the product development lifecycle. By considering power dynamics, incorporating safety concerns into design and testing, and collaborating with support practitioners to build responsive systems, both security researchers and practitioners can reconfigure cybersecurity practices to centre people’s safety in technology design. In other words, abusability offers a framework to build safer online spaces. This chapter offers both a series of recommendations and a maturity model which can be used to evaluate company practices and hold them accountable. This is critically important as online harassment and abuse is a growing problem which causes serious harms, particularly to those who are already marginalised or at risk, and frameworks for evaluating tech company practices which enable abuse are still in their infancy. I also discuss three paradoxes of abusability: the concept has a lot of potential to be useful, but it must be deployed with care and an awareness of how it can channel ideas of tech solutionism, tech determinism, or a wilful ignorance to the political economy of technology production.

Conclusion: From Security to Solidarity

Introduction

I started my thesis aiming towards a feminist cybersecurity – did I find it? Although this evaluation ultimately rests with my readers, in this concluding chapter I lay out my thoughts on this question. I summarise the findings of each preceding chapter, return to answer my research questions (copied below), outline my key contributions, reflect on positionality and limitations, and conclude with future directions for research.

Overarching research question (ORQ): How can we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

- **RQ1:** why do existing security practices fail to account for technology-mediated coercive control?
- **RQ2:** how can we use feminist epistemology and participatory methods to reconfigure security practices?
- **RQ3:** should we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

In short, I believe a truly feminist cybersecurity would no longer be recognisable as 'cybersecurity'—this discipline that emerged from engineering and the military predominantly to protect software and hardware (and their owners), and not "people" (if by people we mean those who are not near the top of any given hierarchy). In seeking to rewire cybersecurity to address the thorny problems of tech abuse, I found the limits of cybersecurity as a framework, as it will always—to some extent—point to technical design solutions rather than structural ones. Likewise, I believe this thesis points to some of the limitations of feminism, particularly feminisms which remain preoccupied with the interpersonal dynamics of injustice and miss or even reinforce the oppression of the carceral state. Hence my thesis is a call to reconfigure cybersecurity towards solidarity.

Chapter Summary

Chapter 2 presents the conceptual framework of the thesis, unpacking and problematising the concept of security, so that subsequent chapters can show how it might be put together differently. I situate my research in ongoing discussions on the nature of (cyber)security, in particular critical and feminist theories of security. I explore how security practices can reinforce unjust power dynamics, particularly in omitting many forms of threat and failing to include women and minoritized groups as valid security subjects. Feminist notions like standpoint theory and intersectionality offer a valuable critique of hegemonic, mainstream

understandings of security, showing how threat models are shaped by unacknowledged positionality. Likewise, applying the lenses of practice and care work can help make visible a wider variety of forms of security work than is commonly acknowledged, allowing for a potential reframing or reconfiguring of security. I explain how my methodology draws on critical and feminist theories and reflects these commitments. Lastly, I introduce the central case study of tech-facilitated coercive control, which reflects both a common omission in security threat-modelling, and a central focus on feminist activism and theory.

Chapter 3 critically examines the cybersecurity method of threat modelling, asking what it can show us about the phenomenon of technologically mediated abuse. A review of forty smart home security analysis papers shows that this threat model is almost entirely absent from the security analysis literature, and where it is considered, the threat model carries implications that are dismissive or implicitly victim-blaming. This illustrates the power of applying feminist critiques to identify gaps and omissions in conventional threat modelling. To address this gap, I adapt the method of threat modelling to account for the context of intimate partner violence, using the case study of a smart lock, to show how researchers or manufacturers could identify design features which facilitate or constrain the possibility of abuse. I also reflect on the limitations that the conventional methodology of threat modelling imposes on thinking about the problem of tech-enabled abuse: by limiting the focus to design changes, and manufacturers' notions of feasibility, we are limited in the scope of solutions and responses we can consider.

Chapter 4 further reconfigures the method of threat modelling, by centring people's experiences in a new method called "participatory threat modelling." I present the evolution of this method throughout twelve in person and online workshops, starting with one-off workshops with the general public and finishing with an extended collaboration with Voice of Domestic Workers. This methodological innovation allows researchers to collaborate with members of the public or specific community groups in the process of problem definition: an approach long established in the field of participatory action research, but new to cybersecurity. This method points the security researcher to intertwined structural threats, such as gendered labour or racialised immigration policy, which might otherwise be perceived as "outside of the scope" of security research. In stark contrast to the method used in Chapter 3, problems like Home Office surveillance of public health records cannot and will not be resolved through design changes. As a counterpart to understanding the underlying causes of security threats as structural, the study also demonstrates the many ways in which meaningful sources of security are communal.

Chapter 5 examines these communal sources of security more closely, through interviews about the security practices of advocates who support survivors of tech abuse. I show how these

practices demonstrate a mixture of emotional and technical expertise, amounting to a unique kind of security expert. I argue these empirical findings call for a conceptual reconfiguring of concepts like "technical expertise" and "cybersecurity experts", so that we can acknowledge and compensate pragmatic forms of expertise which advocates and care workers have developed in their work. These advocates also co-construct networks of care in their communities and broader society, to make more supportive and safer environments for survivors and build safe(r) spaces both on- and offline. This provides a model for a feminist security rooted in care and solidarity. However, many of the practices the advocates describe are more about safety and empowerment than securing devices: suggesting that what they are doing may move beyond the framework of security altogether. Similarly, the concept of care, which still implies power dynamic between care-giver and care-receiver is more hierarchical than the notion of solidarity.

Lastly, Chapter 6 develops the notion of "abusability" based on these tech abuse advocates' ideas on how technology could be improved, as well as the findings from earlier chapters. By considering power dynamics, incorporating safety concerns into design and testing, and collaborating with support practitioners to build responsive systems, both security researchers and practitioners can reconfigure cybersecurity practices to centre people's safety in technology design. I also note some paradoxes and limitations in the concept of abusability. Designing safer technology is an important part of the response to technology abuse, but it is not sufficient on its own, and we must proceed with a cautious awareness about tendencies towards tech solutionism, tech determinism, and perverse incentives within the political economy of technology production.

Research Questions Review

In this section, I return to my research questions:

Overarching research question (ORQ): How can we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

- **RQ1:** why do existing security practices fail to account for technology-mediated coercive control?
- **RQ2:** how can we use feminist epistemology and participatory methods to reconfigure security practices?
- **RQ3:** should we reconfigure cybersecurity practices to account for tech-facilitated coercive control?

My answer to the ORQ can be simplified to a three-step process: first, we must acknowledge widespread limitations in current concepts and practices. Second, we must involve a wide variety of excluded and marginalised groups in defining the threats and problems security

should address. Third, we must collaborate with these groups and the support sector to develop responses with the values of care and solidarity. These collaborations involve a set of conceptual reconfigurings: adopting terms like cybersecurity and threat modelling in order to subvert them, so that a feminist cybersecurity becomes instead a call for solidarity.

First, we must acknowledge serious and widespread limitations within the field of cybersecurity as it is conventionally practiced (as covered by RQ1). As I outline in Chapter 2, the concept of security is often used to defend the status quo, which can mean defending an unjust set of power relations. This operates at the level of language and concepts, as well as in practices of problem framing, and patterns of exclusion or inclusion (who do we imagine as a threat? who do we look to for solutions? whose answer to these questions do we prioritise?) To answer RQ1, cybersecurity as it is currently defined is too narrow. Much of the conceptual language and discourse around security does not allow for problems related to abuse in problem framing. In Chapter 3, I show how by using gender as a category of analysis, critical theory can pinpoint oversights in security analysis. Conventional threat modelling practices tend to omit or invalidate abuse scenarios, sometimes through categorising these instead as "privacy" or "safety" concerns. It may be the case that privacy or safety in fact offer better concepts or paradigms to address abuse scenarios. In fact, some work has begun on "privacy threat modelling" (Wuyts et al., 2014). However, as long as security and cybersecurity is a dominant conceptual framework in technology design, it is a glaring omission to exclude scenarios which are currently causing emotional, psychological, and physical harm to survivors from security threat models.

To counter the broader tendency to prioritise certain kinds of "technical" or "security" expertise, we must centre perspectives from marginalised groups into what we consider to be a threat, and what we consider to be security. Chapter 4 outlines a method, participatory threat modelling, which security research can use to implement this aim, which reflects an understanding, rooted in intersectionality and feminist standpoint epistemology, that through lived experience of oppressive systems, marginalised people have different and, in many cases, more relevant understandings of the systems we need to dismantle and the systems we need to (re)build than we (in the privileged centre) do. As a graduate student at Oxford, I am still writing very much from the privileged centre—I will return to how my (incomplete) awareness of this positionality shapes my research in the reflections section below.

Starting at the level of problem framing helps mitigate some of the risks of including perspectives from disempowered groups without tokenism, however it certainly does not eliminate this dynamic. Therefore, this kind of research needs to be constantly mindful of the

values of solidarity, approaching potential and currently collaborators with the mindset of working to define and respond to a problem together, rather than protecting or defending vulnerable people. This is the core of my answer to RQ2.

Lastly, in developing responses to technology-facilitated abuse, we must collaborate with community groups and the support sector to develop networks of care. My interviews with advocates who support survivors show alternative forms of security and technical expertise which we can learn from. Chapter 6 expands this further, outlining practical steps for including these forms of expertise in technology and security design. Such collaborations draw on and reinforce a set of conceptual reconfigurings. By seeing community support groups as an important source of security, we can build with and on top of these existing sources of security rather than replacing them. By understanding the deeply intertwined psychological, emotional, and technical forms of expertise that are necessary to support survivors, we can discard narrow ideas of technical experts.

This brings me to the final question R3, i.e., *should* we attempt to reconfigure cybersecurity, or would it be better to do away with notions of technical expertise and (cyber)security altogether? I believe, in the long run, we should move past cybersecurity. It would both be more practical and more just if we had a clear understanding of where we are speaking of "machine integrity" (i.e., a technology or system is doing what it is designed) and where the concern is "human safety" and not assume one guarantees the other. As Dunn Cavelty (in Dwyer et al. 2022) says, "A critical cybersecurity must stop being about cybersecurity to do its best work yet." However, this thesis adopts these terms, and speaks this language, with the awareness that these terms currently still carry a lot of legitimacy and even hegemony. Using these terms allows me entry into certain conversations (entry into a funded PhD programme, for example, or publications like USENIX) while also challenging to what these terms mean. As Dwyer et al. (2022) note, using this language allows critical researchers to maintain relevance and access to mainstream "security" conversations. This thesis adopts terms like cybersecurity and threat modelling to subvert them, so that a feminist cybersecurity becomes a call for solidarity. This is a discursive move which supports the aim of broadening security to eventually displace it. Making cybersecurity "feminist", i.e., making it care about groups which are marginalised and face higher risk, is a step towards this, by building solidarity between researchers and communities working to build more just societies.

At the time of writing, the people, expertise, resources, and agenda-setting power of the term "cybersecurity" is significant enough that I believe it is worth constructively engaging with, while limiting its harms, rather than attempting to bypass or abolish it altogether. Many people

enter computer science, engineering, and cybersecurity out of a genuine desire to build better worlds, or to make the current world safer. I believe these kinds of good intentions are hindered by a widespread lack of power analysis and reflexivity in cybersecurity and the broader tech industry. My pragmatism is also due to the pressing nature of the problem of tech-enabled abuse: if cybersecurity offers some tools and resources to address the issue, it is important to work with the existing concepts, industry, practitioners, etc. while simultaneously trying to reform cybersecurity. Ultimately, I take a pragmatic stance with the hope of paving the way for a more radical change in the future.

Contributions

My work carries a variety of critical implications, with relevance for academic researchers, advocates, technologists, and policy makers. This section summarises these according to theoretical, methodological, empirical, and practical contributions.

Theoretical

My work draws on an important theoretical lineage stretching from critical and feminist security, intersectional feminism, and design justice (Coles-Kemp et al., 2018a; Constanza-Chock, 2020; Crenshaw, 1991; Robinson, 2011; Tickner, 1993). I build on this tradition alongside a crucial emerging shift in cybersecurity towards research working with marginalised groups (Geeng et al., 2022; Wang, 2018; Warford et al., 2022). My work contributes a conceptual framework for reconfiguring cybersecurity (copied below) and an in-depth application of feminist standpoint epistemology to cybersecurity research. The feminist notion that the perspectives of marginalized and/or oppressed individuals can help to create more objective accounts of the world has critical importance for cybersecurity (Harding, 2001). This conceptual framework opens up space for new methods, findings, and conceptions of security within this field.

	Current paradigm	**Reconfiguring**
What does cybersecurity protect?	Machine, information, and networks (by extension – their owners)	People embedded in networks of social relations
Who does it protect it from?	Hackers and thieves (external actors)	Other people – particularly those in intimate spheres and positions of power

What damage/harm is important?	Financial cost determined through risk assessments	Suffering (emotional and psychological harm) and reinforcing unjust systems of power
Which methods does cybersecurity use?	Technical analysis, developing security measures (such as access controls)	Participatory and reflexive methods (such as participatory threat modelling)

Table 1: Reconfiguring cybersecurity

I also show that using gender as a category of analysis can help us pinpoint oversights in security analysis. Incorporating positionality and structural power dynamics can allow cybersecurity research to be critical and self-aware of how these power dynamics shape our research through omission, designating those in power as worthy security subjects and those with less power as potential threats. My work also strengthens findings which show that threat modelling with marginalised people points to community support networks and structural insecurity. By drawing on feminist methods and shifting focus from securing property to solidarity with marginalised groups, security research can counterbalance these power dynamics. My work has already informed research in cyber law, application security, and cyber policy which seeks to apply feminist lenses to privacy and security issues .

In attempting to reconfigure cybersecurity to make it fit for purpose in defending against threats like technology-enabled coercive control, I also identify the benefits and limitations of cybersecurity as framework for responding to digital problems. In this way, I contribute to ongoing theoretical discussions within critical cybersecurity studies on the nature of (cyber)security—what it is and what it should be. I chart how participatory threat modelling tends to point to solutions based on changing broader structures which create insecurity, rather than technical solutions which aid individual security. This is both a methodological and an epistemic contribution: who gets to define threats in security research changes not only the content of security recommendations but also the underlying concept of security that is contained in them.

This work also leads me to reframe much of the current computer science research on technology-facilitated abuse, which often treats this phenomenon as a private matter, stemming primarily from interpersonal violence. Feminist security theorists will find value in my work as it demonstrates that methods of analysis, such as using gender to understand omissions in

security, can apply to the relatively new domain of cybersecurity. However, my work expands this focus not just to coercive control (drawing on violence research in feminist sociology) but also to considering state sanctioned forms of surveillance, stalking and abuse. Survivors of intimate partner violence face many similar threats to targets of state surveillance: constant surveillance; use of intimate data to threaten, coerce and discredit; and a need to keep up to date with evolving technologies like spyware and constantly changing platform privacy policies. Some—like immigrant women—face both forms of threat at once, alongside other threats from labour exploitation, online harassment. Researchers working on feminist cybersecurity cannot limit themselves solely to thinking about gender and must consider intersecting forms of oppression at both the personal and structural levels of analysis.

I also define the concept of "networks of care" – i.e., networks of practitioners willing and able to support survivors through developing more supportive environments—and demonstrate their importance in developing communal forms of digital security. Through close attention to these advocates' security and care practices, I make an empirical contribution to understanding how technical and psychological expertise is critical for meaningful digital security. Standpoint epistemology produces a different understanding of where security comes from, resulting in a call to action for security researchers to apply this method and practice a different kind of security.

Crucially, although some of the work advocates do resembles that of conventional security practitioners (risk assessment, threat modelling, securing accounts), the support they offer also deals with the tricky emotional and psychological aspects of abuse: gaslighting and perceived expert status of abusers, and survivors' needs for validation and emotional support. Returning again to feminist epistemology, I argue these networks of care are an important source of technical and security expertise. Critical security theorists looking for positive forms of security can learn from this: look for alternative forms of security not in military and corporate defence but among care workers and advocates. Paradoxically, these advocates rarely adopt the language of security themselves, often speaking instead of safety, empowerment, or even freedom. Conscious of the risks of care—which can impose a hierarchical relationship between care-giver and care-receiver—a focus on empowerment and solidarity can allow both researchers and practitioners to approach these important problems while respecting the agency and expertise of those most severely affected by them.

Lastly, I develop the concept of abusability and identify and address potential problems in the concept, such as technological solutionism, determinism, and a wilful ignorance of the political

economy of the tech industry. In expanding and interrogating abusability, I put forward new possibilities for holding companies accountable for enabling abuse.

Methodological

This thesis develops several key methodological innovations. In Chapter 2, I combine existing intimate partner violence research with the cybersecurity method of threat modelling, adapting this method to suit various forms of technology-enabled abuse. This opens the door wider for security researchers and technology designers to anticipate and mitigate a wide variety of sociotechnical threats often omitted in conventional threat modelling. I then develop this further with pragmatic recommendations on incorporating abusability in product design and collaborating with the support sector to develop responsive systems. This comes at a crucial time when Trust and Safety teams in tech companies are belatedly gaining more power to influence design decisions and implement these design methods before harmful technology is released (Macgillivray & Wong, 2020). I believe industry practitioners working on online harms and Trust and Safety will find a lot of practical use in my innovations in threat modelling, thoughts on incorporating abusability in the product design life cycle and collaborating with support services in a respectful and fair way.

I then further extend the method of threat modelling with a methodological innovation titled participatory threat modelling (PTM). Although many people have worked threat modelling with marginalised and at-risk groups (Kazansky, 2021), to my knowledge our work is the first formal application of this practice as a research method. Applying feminist participatory methods to threat modelling in an iterative process across 14 months, I propose a way researchers can involve various groups traditionally excluded from threat modelling (i.e., anyone who isn't a security researcher) to define their own threats, develop more robust threat models while encouraging and enabling participants to take action to defend themselves online. These workshops created environments for mutual learning, safe(r) spaces for discussing difficult topics, and combined research with skill-sharing and empowerment. Sharing a workshop with others with similar experiences allowed groups like survivors of image-based sexual abuse to develop solidarity around shared experiences.

The methods we developed—and disseminated in a freely accessible online report—can benefit a wide variety of community groups seeking to develop their digital privacy and self defence capacity. This also provides a model for less extractive forms of usable security and privacy research with excluded or marginalised groups, which is an area of increased interest in computer science research. I expanded on other methods for participatory research—like

participatory data analysis in "walkthroughs" or the option to opt out of data collection while participating in workshop discussions—which are rarely used in security research but would be highly beneficial.

In collaboratively developing a digital privacy and security guide for migrant domestic workers, we also developed the idea of security advice as method: by including MDW's advice for other workers, as well as using their questions and reported threats as the basis for our own desk-based research, which strengthened both an academic threat model and the pragmatic guide itself. Technology researchers in security and human-computer interactions can benefit significantly from applying such participatory methods. More broadly, I believe this works as a useful model for collaboratively developing and disseminating research findings that are useful to participants' communities and not just academic publications.

These forms of methodological innovation and experimentation offered ways to explore underlying concepts like security, care, and solidarity (Aradau, 2014). For example, collecting information through advice and questions asked by migrant domestic workers into the security guide highlighted questions of where we trusted our own instinct as security researchers, where we were prepared to have our expectations and assumptions challenged, and, in this process, how security expertise can be developed collaboratively. Trying to run workshops in a way that was supportive to participants and sustainable for tech support volunteers highlighted the tricky labour aspects of care. And the questions of how labour, ownership, and authorship was distributed among academic and peer research highlighted questions of solidarity across very different social standpoints.

Empirical

My work offers several key empirical contributions. In Chapter 5, I offer a detailed documentation of security practices among tech abuse advocates, providing a rich analysis of intertwined technical & emotional support practices. In doing so, I counter what I describe as a deficit model for research: looking for what needs fixing, but not looking at innovation that is happening among practitioners and what we can learn from it. This also offers a pragmatic alternative to prioritising new technical solutions. These descriptions will be of use to those in academic research, advocacy, and tech companies (for example, those improving customer support lines) who hope to provide support to users affected by abuse, as they serve as a documentation of best practices. I believe these findings will be useful to those seeking to develop capacity in the advocacy sector and among social workers to better prepare them to support those experiencing technology abuse. For example, advocates consider intersecting

systems of power and oppression, like misogyny, racism, or ableism, in their threat assessment; these factors should be considered in security threat assessments more broadly.

Many of these best practices would also be helpful in providing support for *all* technology users, whether or not they are experiencing abuse. These empirical descriptions are also useful for validating feminist security theory empirically: many feminist theories call for more focus on care, emotion, and human safety in masculinised fields of technology and security. By providing an empirical study of what such practices look like, these suggestions moved from theoretical alternatives to demonstrable evidence.

I also documented advocates' recommendations for how technology design could be different, including more funding and resources for capacity building in law enforcement and the support sector, product design in which safety and security are built in by default, and better responsiveness when advocates and survivors raise problems. These recommendations are grounded in an understanding of security as networked and relational: to adequately respond to the evolving problem of tech abuse, tech companies and security workers need to develop respectful relationships with advocates working on these problems on the ground. Their recommendations are valuable as advocates' expertise on technology safety has often not been included in privacy and security discussions. Building on these recommendations, I develop a maturity model for abusability, which could be used by activists or researchers to evaluate company practices and hold companies accountable. It can also be used by advocates in deciding whether or not to partner with any given company.

Furthermore, I offer detailed threat models for various at-risk groups, such as survivors of intimate image abuse, activists, and migrant domestic workers. Examples such as the case of dating abuse where men will threaten to report workers to immigration authorities show how various threats—such as precarious immigration status and gendered harassment—are interconnected and reinforcing. These findings lead to a variety of specific design implications as well as better models for how different identity-based threats intersect. These will be valuable for technology researchers in security and human-computer interaction as well as designers in industry. These design implications also carry important messages for policymakers, particularly regarding the importance of legislating for better data sharing on online harms from technology manufacturers, as such data will be necessary to validate threat models for abuse and design safer technology.

Practical and engaged

To engage with different audiences such as academics, practitioners, policymakers, and the general public, I shared my research in a variety of ways. I presented at a variety of social and technical conferences, including the Conference on Human-Computer Interaction (CHI); the International Studies Association (ISA), the Privacy Engineering, Practice, and Respect; and the USENIX Privacy and Security Conference. I organised a panel with intimate partner violence practitioners at Rights Con (a digital rights conference) and spoke on a panel on online misogyny at the Shameless! Festival of Activism Against Sexual Violence. I also spoke on the BBC World Digital Planet radio programme. Alongside practitioners, I co-authored a piece for the United Nations Institute for Disarmament Research (Slupska et al., 2021) and participated in a policy retreat organised by the Foreign and Commonwealth Office at Wilton Park (Wilton Park, 2022).

My work also contains a set of very pragmatic contributions, notably the digital privacy and security guide for migrant domestic workers, as well as the Reconfigure report and Abusability toolkit. These non-academic publications engage directly with various practitioner audiences as well as community groups which seek to improve their digital privacy and security practices.

Reflections and limitations

This thesis started out as a search for a feminist cybersecurity and ends in a call for empowerment and solidarity. This trajectory is deeply shaped by my positionality; in this section I reflect on some of my original motivations for undertaking this work as well as limitations in this project. Knowing that I and others I care about have experienced gendered harm and feelings of powerlessness, I wanted to use my position of relative power and influence as a researcher at an elite institution to help build better systems for creating security for people experiencing violence. The origins of the project therefore stem from a feminist solidarity and shared experiences of harm. However, as I have discussed in previous reflections on positionality (in Chapter 2 and Chapter 4), notions of positionality which focus only on experiences of harm rather than privilege are incomplete. Therefore, in this final reflection section, I will focus in two ways my position within a specific discipline and institution shaped my work.

Cybersecurity Framework

My position within a cybersecurity programme—which is also the source of my funding—has both made this work possible and imposed a specific mould. Being in this programme made it more likely that my work would be framed around cybersecurity as a concept, and oriented around fixing, improving or reforming cybersecurity (for example, by making it more "feminist") rather than resisting it altogether. As Dwyer et al. (2022) point out in their reflections on critical cybersecurity, "As scholars, we are complicit in giving cybersecurity more power than it arguably should have. We have used it as a label to create an identity for ourselves." This label gives access to certain conversations (particularly in policy and design spaces) as well as routes to funding (as my PhD shows). Dwyer et al. (2022) argue that a "a critical cybersecurity project may be more of an un-doing [...] how can [this project] destabilize power structures and challenge inequalities, for example, even if this means *undoing* the narratives of cybersecurity?" My work offers an answer to this question, as well as to their calls to theorise and understand emergent relations between technology and communal living.

However, in adopting a cybersecurity framework, I also adopt many of the limitations that Dwyer et al. (2022) and others have critiqued. For example, I adopt the language of "threat" and "threat modelling" which furthers a sense of insecurity (Dwyer et al., 2022; Kazansky, 2021). Rather than doing away with the language of threat altogether, I describe problems like intimate partner violence and immigration surveillance using the language of threat modelling. This is, in a way, destabilising of certain power structures, as the language of threat has historically been more likely to describe e.g., domestic workers and immigrants rather than used *by* them. But it risks recreating a sense of constant insecurity, particularly for marginalised groups (Kazansky, 2021). There is a trade-off here, with access to wider cybersecurity and tech discussions (discussed earlier). As I argued earlier, in the long run it is likely better to do away with notions of (cyber)security altogether. Although I see my work as a step in this direction, the extent to which I have adopted this language is also a limitation for this thesis.

Eurocentricity

Throughout the chapters of my thesis, I course-correct from focusing only on my own analysis (looking at smart home security papers), to including voices from my wider community (in feminist security workshops), to intentionally partnering with people with very different standpoints to my own (migrant domestic workers in the UK and tech abuse advocates in different countries). This is a conscious attempt to avoid the common pitfalls of white feminism:

i.e., generalising from white womens' experiences. However, although my work at times purports to centre marginalised voices (particularly in proposing the method of participatory threat modelling), this is true only relative to the broader field of cybersecurity. Ultimately my work—like most if not all PhDs—centres my own voice much more than anyone else's.

Writing as I am from the privileged centre, I am not fully aware of the omissions I am making because of this position. A core limitation is certainly the Eurocentricity of my work: with the exception of the project with migrant domestic workers, the majority of people I spoke with or interviewed for this work, and the majority of the work I draw on, are from WEIRD (Western, educated, industrialized, rich and democratic) countries and particularly the US and UK. This recreates a major limitation in most scholarship on tech abuse and cybersecurity. In fact, the project of reconfiguring cybersecurity may not be recognisable or necessary outside of my specific context—as Dwyer et al. (2022) note, "even in its most positive, emancipatory, or "social security" guises [...], there is still something troubling me about the kinds of places and forms of life that cybersecurity practices and discourses centre on, so that it makes me wonder if it is possible for a critical cybersecurity to be truly 'un-Eurocentric.'" As Jairo Funez (2022) has written, Eurocentricity allows academics to ignore how colonialism and racism, ongoing extraction of materials from the majority world to the minority world constitute modernity. These dynamics are certainly visible in cybersecurity: as Dwyer et al (2022) outline, some have already started to document this.

One way this influenced my work is in the underlying assumptions behind the "we" in my ORQ , RQ2, and RQ3. When I say "we", there is a risk of assuming this means researchers "like me", i.e., progressive, justice-oriented, situated in the Global North, studying technology or security, etc. When I speak of solidarity *with* marginalised people, learning *from* marginalised people, I at times implicitly exclude them from this project of reconfiguring cybersecurity, as I do not think of these communities as a primary audience for this thesis. However, the approach of participatory research means that marginalised groups are both existing and potential future research collaborators. We should reject a binary of "us" (researchers) helping "them" (marginalised people).

Another way I may be contributing to this issue is by describing certain dynamics (for example, failures to include threats faced by women or migrant domestic workers in the home) as "omissions" rather than as constitutive of cybersecurity (Bilgin, 2010). I maintain that notions of security can be more flexible, and open to a tactical reconfiguring: migrant domestic workers and other marginalised groups want and deserve security (or perhaps simply "peace of mind")

too—security does not need to be only for maintaining the wealth and power of the rich and powerful.

The positionality of migrant domestic workers—migrants from the majority world in the global north—is particularly important given the Eurocentricity of my work and the broader field. For example: the contrast between our expectations that their threat model would mostly relate to employer surveillance, and their ranking of Home Office surveillance as the most pressing source of threat, points to the harms and insecurity created by institutions promising to create security. It also highlights the importance to listening at the problem-framing stage rather than asking questions limited by researchers' understanding of threats. However, the migrant domestic workers we partnered with are still based in the Global North/minority world, and their interests and problems will differ from those physically located in the majority world. As always, it is important to keep asking, "who is *not* in the room?" These are limitations which future work can and should build upon.

Future directions

This thesis helps put into motion an emerging direction in cybersecurity research: one which is justice-oriented, reflexive, and engaged in solidarity with communities (Geeng et al., 2022; Wang, 2018; Warford et al., 2022). Some have described this as "the inclusive turn" (Wang, 2018) or an increased focus on "at-risk user research"(Warford et al., 2022). Future directions for this research should continue to combine the pragmatic focus of engineering and computer science (a desire to build systems and find solutions) with the greater reflexivity and social awareness of social science research. A brilliant recent example is Owens et al.'s (2022) work on immigration tracking applications, which combines qualitative research on review comments with a technical analysis which shows that these applications include ad libraries. This provides evidence that companies may be profiting from compulsory use of carceral surveillance systems. This kind of research would apply the mindset of abusability more broadly, asking what kinds of technologies and uses should we restrict? Such work necessarily includes a focus not just on *building* better technical systems, but also on uncovering the operations of existing, harmful socio-technical systems, to dismantle or abolish them (Kamara, 2020): this is an area where both computer scientists and social scientists can contribute immensely by working together.

Much work remains in implementing abusability practices and evaluating companies' implementations. The field needs to develop frameworks and industry standards for evaluating the abusability of existing systems and the extent to which developers account for abusability in

design. Further work remains in fleshing out our maturity model for abusability. In addition to further research on Facebook and other companies' efforts to address image-based sexual abuse, I believe my work opens many routes into examining abusability design in the tech industry.

I aim to continue to develop the partnership with Voice of Domestic Workers to better understand and implement their ideas for safety and justice in immigration and domestic work. I would also like to see and contribute to the expansion of clinics such as the Clinic to End Tech Abuse in New York and the Coercive Control Initiative in Seattle, which can keep technology and security research grounded in everyday people's problems. More broadly, my work is call for technology and security researchers to partner with local community organisations focused on justice and safety to support their work, building on, and expanding existing networks of care. Much existing research has focused on defining threats and problems; there is much more work to be done to understand and adopt survivors' and marginalised groups' positive ideas of safety, security, and justice. Future work should also engage more critically with questions of access: who can access tech abuse support services and whom do they exclude?

Social structures like misogyny, racism, and borders create more insecurity than technical vulnerabilities. As security and technology researchers, we must dismantle the technologies that enable these forms of abuse and look to build new socio-technical systems based on care and solidarity. My thesis offers both a conceptual framework and a methodology to support a shift that is already ongoing in computer science and information security, towards working with oppressed groups and against oppressive systems. Social science and computer science researchers can use the concepts and methods I have developed to advance justice-oriented technology research.

My thesis provides an opening for understanding what this solidarity might look like in practice. Much work remains to flesh out this concept of solidarity. How do we manage distributional conflicts, situations where one person's safety makes another feel more unsafe? What would an internet built with care and solidarity (rather than cybersecurity) look like? To echo Srinivasan (2022), we do not know; let us try and see.

Bibliography

A. J. Neumann, N. S. and R. D. W. (1977). *Post-processing audit tools and techniques*. US Department of Commerce, National Bureau of Standards. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf

Åhäll, L. (2016). The dance of militarisation: a feminist security studies take on 'the political.' *Critical Studies on Security*, *4*(2). https://doi.org/10.1080/21624887.2016.1153933

Akiwowo, S. (2020). Digital Self Care. In *Fix the Glitch*. https://fixtheglitch.org/digitalselfcare/

Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021). Collective information security in large-scale urban protests: The case of Hong Kong. *Proceedings of the 30th USENIX Security Symposium*.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*. https://doi.org/10.1108/JSIT-02-2018-0028

Aradau, C. (2014). Critical Security Methods. In *Critical Security Methods*. https://doi.org/10.4324/9781315881549

Aradau, C., Huysmans, J., Neal, A., & Voelkner, N. (2014). Critical security methods: New frameworks for analysis. In *Critical Security Methods: New Frameworks for Analysis*. https://doi.org/10.4324/9781315881549

Arias López, B. E., Andrä, C., & Bliesemann de Guevara, B. (2021). Reflexivity in research teams through narrative practice and textile-making: *Https://Doi.Org/10.1177/14687941211028799*. https://doi.org/10.1177/14687941211028799

Arief, B., Coopamootoo, K. P. L., Emms, M., & Moorsel, A. van. (2014). Sensible privacy: How we can protect domestic violence survivors without facilitating misuse. *Proceedings of the ACM Conference on Computer and Communications Security*. https://doi.org/10.1145/2665943.2665965

Bardzell, S. (2010). Feminist HCI : Taking Stock and Outlining an Agenda for Design. *CHI*. https://doi.org/10.1145/1753326.1753521

Bellini, R., Forrest, S., Westmarland, N., & Smeddinck, J. D. (2020). Mechanisms of Moral Responsibility: Rethinking Technologies for Domestic Violence Prevention Work. *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13.

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., & Uebelacker, S. (2015). Maybe poor johnny really cannot encrypt - The case for a complexity theory for usable security. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2841113.2841120

Benjamin, R. (2019a). *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life* (R. Benjamin, Ed.). Duke University Press. https://www.dukeupress.edu/captivating-technology

Benjamin, R. (2019b). Race After Technology: Abolitionist Tools for the New Jim Code. *Social Forces*. https://doi.org/10.1093/sf/soz162

Bernd, J., Abu-Salma, R., & Frik, A. (2020). Bystanders' privacy: The perspectives of nannies on smart home surveillance. *FOCI 2020 - 10th USENIX Workshop on Free and Open Communications on the Internet, Co-Located with USENIX Security 2020*.

Bernstein, E. (2012). Carceral politics as gender justice? The "traffic in women" and neoliberal circuits of crime, sex, and rights. *Theory and Society*. https://doi.org/10.1007/s11186-012-9165-9

Bhalerao, R., Hamilton, V., McDonald, A., Redmiles, E. M., & Strohmayer, A. (2022). Ethical Practices for Security Research with At-Risk Populations. *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 546–553. https://doi.org/10.1109/EUROSPW55150.2022.00065

Bilgin, P. (2010). The 'Western-Centrism' of Security Studies: 'Blind Spot' or Constitutive Practice? *Http://Dx.Doi.Org/10.1177/0967010610388208*, *41*(6), 615–622. https://doi.org/10.1177/0967010610388208

Bishop, E. C., & Shepherd, M. L. (2011). Ethical reflections: examining reflexivity through the narrative paradigm. *Qualitative Health Research*, *21*(9), 1283–1294. https://doi.org/10.1177/1049732311405800

Blythe, M., Andersen, K., Clarke, R., & Wright, P. (2016). Anti-solutionist strategies: Seriously silly design fiction. *Conference on Human Factors in Computing Systems - Proceedings*, 4968–4978. https://doi.org/10.1145/2858036.2858482

Bondi, L. (2008). On the relational dynamics of caring: A psychotherapeutic approach to emotional and power dimensions of women's care work. *Gender, Place and Culture*, *15*(3). https://doi.org/10.1080/09663690801996262

Bowen, R., Hodsdon, R., Swindells, K., & Blake, C. (2021). Why Report? Sex Workers who Use NUM Opt out of Sharing Victimisation with Police. *Sexuality Research and Social Policy*, *18*(4), 885–896. https://doi.org/10.1007/S13178-021-00627-1/FIGURES/1

Braun, V., & Clarke, V. (2020). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Https://Doi.Org/10.1080/14780887.2020.1769238*, *18*(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). Thematic analysis. In *Handbook of Research Methods in Health Social Sciences*. https://doi.org/10.1007/978-981-10-5251-4_103

Brown, M. L., Reed, L. A., & Messing, J. T. (2018). Technology-based abuse: Intimate partner violence and the use of information communication technologies. In *Mediating misogyny* (pp. 209–227). Palgrave Macmillan, Cham.

Browne, S. (2015). *Dark matters: on the surveillance of blackness*. Duke University Press.

Bueger, C. (2016). Security as practice. In T. Balzacq & M. D. Cavelty (Eds.), *Routledge Handbook of Security Studies: Second Edition* (2nd ed., pp. 1–479). Taylor and Francis. https://doi.org/10.4324/9781315753393

Cafolla, A. (2017). *Facebook wants your nudes to tackle revenge porn | Dazed*. https://www.dazeddigital.com/science-tech/article/38003/1/facebook-wants-your-nudes-to-tackle-revenge-porn

Calderon, A., Taber, D., Qu, H., & Wen, J. (2019). *AI Blindspot*.

Calton, J. M., Cattaneo, L. B., & Gebhard, K. T. (2016). Barriers to Help Seeking for Lesbian, Gay, Bisexual, Transgender, and Queer Survivors of Intimate Partner Violence. *Trauma, Violence, and Abuse*, *17*(5), 585–600. https://doi.org/10.1177/1524838015585318

Cao, S. (2017). *Send Nudes? Facebook Wants Your Naked Pics to Prevent Revenge Porn | Observer*. Observer. https://observer.com/2017/11/facebook-using-hashing-technology-to-help-prevent-revenge-porn/

Centre for Women's Justice. (2020). *Police officers allowed to abuse with impunity in the 'locker-room' culture of UK forces, super-complaint reveals — Centre for Women's Justice*. https://www.centreforwomensjustice.org.uk/news/2020/3/9/police-officers-allowed-to-abuse-with-impunity-in-the-locker-room-culture-of-uk-forces-super-complaint-reveals

CETA. (n.d.). *CETA | Resources*. Retrieved February 24, 2022, from https://www.ceta.tech.cornell.edu/resources

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

Chen, C., Dell, N., & Roesner, F. (2019). Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors | USENIX. *28th USENIX Security Symposium (USENIX Security 19)*. https://www.usenix.org/conference/usenixsecurity19/presentation/chen

Citron, D. K. (n.d.). A New Compact for Sexual Privacy. *William & Mary Law Review*.

Clark, A. (2011). Domestic Violence, Past and Present. *Journal of Women's History*. https://doi.org/10.1353/jowh.2011.0032

Coles-Kemp, L., Ashenden, D., & O'Hara, K. (2018a). Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance*, *6*, 41–48. https://doi.org/10.17645/PAG.V6I2.1333

Coles-Kemp, L., Ashenden, D., & O'Hara, K. (2018b). Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*. https://doi.org/10.17645/pag.v6i2.1333

Collins, P. H. (1990). *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. Routledge. https://doi.org/10.2307/2074808

Connolly, D., Aldridge, A., Davies, E., Maier, L. J., Ferris, J., Gilchrist, G., & Winstock, A. (2021). Comparing Transgender and Cisgender Experiences of Being Taken Advantage of Sexually While Under the Influence of Alcohol and/or Other Drugs. *Journal of Sex Research*, *58*(9), 1112–1117. https://doi.org/10.1080/00224499.2021.1912692

Constanza-Chock, S. (2020). Design Justice. In *Design Justice* (Vol. 100, Issue 10). The MIT Press. https://doi.org/10.2105/AJPH.2009.186445

Costanza-Chock, S. (2018). Design Justice: towards an intersectional feminist framework for design theory and practice. *DRS2018: Catalyst*. https://doi.org/10.21606/drs.2018.679

Cramer, F. (2015). What is 'post-digital'? In *Postdigital Aesthetics: Art, Computation and Design*. https://doi.org/10.1057/9781137437204_2

Crawford, K., & Gillespie, T. (2016). What is a flag for? Social media reporting tools and the vocabulary of complaint. *New Media and Society*, *18*(3), 410–428. https://doi.org/10.1177/1461444814543163

Crenshaw, K. (1989). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics. *University of Chicago Legal Forum*, *1989*(1). https://doi.org/10.4324/9780429500480-5

Crenshaw, K. (1991). Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Source: Stanford Law Review*, *43*(6), 1241–1299. https://about.jstor.org/terms

Cruz, M. R. (2008). What If I Just Cite Graciela? Working Toward Decolonizing Knowledge Through a Critical Ethnography: *Qualitative Inquiry*, *14*, 651–658. https://doi.org/10.1177/1077800408314346

Cuomo, D., & Dolci, N. (2019). Gender-Based Violence and Technology-Enabled Coercive Control in Seattle: Challenges & Opportunities. *TECC Whitepaper Series*.

Dabiri, E. (2021). *What white people can do next : from allyship to coalition* (1st ed.). Penguin . https://www.penguin.co.uk/books/443684/what-white-people-can-do-next-by-dabiri-emma/9780141996738

Davis, A. (1981). *Women, Race and Class*. Random House Inc.

Davis, A. (2021). *Strengthening Our Efforts Against the Spread of Non-Consensual Intimate Images | Meta*. Meta. https://about.fb.com/news/2021/12/strengthening-efforts-against-spread-of-non-consensual-intimate-images/

Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics and International Affairs*. https://doi.org/10.1017/S0892679418000618

Devries, K. M., Mak, J. Y. T., García-Moreno, C., Petzold, M., Child, J. C., Falder, G., Lim, S., Bacchus, L. J., Engell, R. E., Rosenfeld, L., Pallitto, C., Vos, T., Abrahams, N., & Watts, C. H. (2013). The global prevalence of intimate partner violence against women. In *Science*. https://doi.org/10.1126/science.1240937

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/1124772.1124861

Dhamoon, R. K. (2013). Feminisms. In Georgina Waylen, Karen Celis, Johanna Kantola, & S. Laurel Weldon (Eds.), *The Oxford Handbook of Gender and Politics* . Oxford University Press. https://doi.org/10.1093/OXFORDHB/9780199751457.013.0003

Domestic CCTV systems - guidance for people using CCTV | ICO. (n.d.). Retrieved July 13, 2022, from https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/

Doty, R. L. (2007). Immigration and the politics of security. *Https://Doi.Org/10.1080/09636419808429375*, *8*(2–3). https://doi.org/10.1080/09636419808429375

Dubler, J., & Lloyd, V. (2019). Break Every Yoke: Religion, Justice, and the Abolition of Prisons. In *Journal of Law and Religion* (Vol. 36, Issue 2). Oxford University Press,. https://doi.org/10.1017/JLR.2021.18

Dupuis, A., & Thorns, D. C. (2017). Home, Home Ownership and the Search for Ontological Security: *Http://Dx.Doi.Org/10.1111/1467-954X.00088*, *46*(1), 24–47. https://doi.org/10.1111/1467-954X.00088

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What Can a Critical Cybersecurity Do? *International Political Sociology*, *16*(3), 1–26. https://doi.org/10.1093/IPS/OLAC013

Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing. In *The International Encyclopedia of Gender, Media, and Communication*. https://doi.org/10.1002/9781119429128.iegmc009

Enloe, C. (1989). Gender Makes the World go Round. In *Bananas, Beaches & Bases. Making Feminist Sense of International Politics.*

Enloe, C. (2012). Foreword. *Sage*, *5*(3), 1–2. https://doi.org/10.1080/15423166.2010.768123567622

Enloe, C. (2019). *Bananas, Beaches and Bases*. https://doi.org/10.1525/9780520957282

Faye, S. (2021). *The transgender issue: an argument for justice* (Vol. 1). Penguin Books Ltd.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology* , 185–200. https://doi.org/10.1007/s10676-006-0001-7

for Cyber Safety, C., & Education. (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. *Frost & Sullivan in Partnership with Booz Allen Hamilton for ISC2*.

Fox, J., & Tang, W. Y. (2017). Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies. *New Media and Society*. https://doi.org/10.1177/1461444816635778

Fox, S., Merrill, N., Wong, R., & Pierce, J. (2018). Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proceedings of the ACM on Human-Computer Interaction*. https://doi.org/10.1145/3274408

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). ``Is my phone hacked?'' Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW). https://doi.org/10.1145/3359304

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact*. https://doi.org/10.1145/3134681

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018a). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. https://doi.org/10.1145/3173574.3174241

Freeman, J. (1972). The Tyranny of Stuctureless. *The Second Wave*, *2*(1). https://www.jofreeman.com/joreen/tyranny.htm

Friedman, B., & Kahn, P. (2002). Value sensitive design: Theory and methods. *University of Washington Technical*.

Friedman, B., Kahn, P. H., & Borning, A. (2009). Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*. https://doi.org/10.1002/9780470281819.ch4

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The power of interpretation: Qualitative methods in cybersecurity research. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3339252.3341479

Fuller, M., Jenkins, M., & Tjølsen, K. (2017). Security Analysis of the August Smart Lock. *Massachusetts Institute of Technology*, 1–16.

Gallotti, M. (2015). Migrant Domestic Workers Across the World: Global and regional estimates. *International Labour Organization (ILO)*. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---migrant/documents/briefingnote/wcms_490162.pdf

Gangadharan, S. P. (2019). *Technologies of control: we have to defend our right of refusal | LSE Business Review*. https://blogs.lse.ac.uk/businessreview/2019/06/22/technologies-of-control-we-have-to-defend-our-right-of-refusal/

Gatenby, B., & Humphries, M. (2000). Feminist participatory action research. *Women's Studies International Forum*, *23*(1). https://doi.org/10.1016/S0277-5395(99)00095-3

Geeng, C., Harris, M., Redmiles, E., & Roesner, F. (2022, August). "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. *31st USENIX Security Symposium (USENIX Security 22)*. https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

Geeng, C., & Roesner, F. (2019). Who's in control?: Interactions in multi-user smart homes. *Conference on Human Factors in Computing Systems - Proceedings*, *13*. https://doi.org/10.1145/3290605.3300498

Glass, N., Clough, A., Case, J., Hanson, G., Barnes-Hoyt, J., Waterbury, A., Alhusen, J., Ehrensaft, M., Grace, K. T., & Perrin, N. (2015). A safety app to respond to dating violence for college women and their friends: The MyPlan study randomized controlled trial protocol. *BMC Public Health*. https://doi.org/10.1186/s12889-015-2191-6

Glass, N. E., Clough, A., Messing, J. T., Bloom, T., Brown, M. L., Eden, K. B., Campbell, J. C., Gielen, A., Laughon, K., Grace, K. T., Turner, R. M., Alvarez, C., Case, J., Barnes-Hoyt, J., Alhusen, J., Hanson, G. C., & Perrin, N. A. (2021). Longitudinal Impact of the myPlan App on Health and Safety Among College Women Experiencing Partner Violence. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260521991880

Goodfellow, M. (2020). *Hostile environment: How immigrants became scapegoats* (2nd ed., Vol. 1). Verso Books.

Gorz, A. (1967). *Strategy for labor; a radical proposal*. Beacon Press. https://www.worldcat.org/title/strategy-for-labor-a-radical-proposal/oclc/236749

Gould, N. (2015). Reflexivity. In *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*. https://doi.org/10.1016/B978-0-08-097086-8.28075-6

Gray, K. L. (2012). Intersecting oppressions and online communities: Examining the experiences of women of color in Xbox Live. *Information Communication and Society*, *15*(3). https://doi.org/10.1080/1369118X.2011.642401

Green, R., & Gilman, M. (2020). The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization. *NYU Review of Law & Social Change*, *42*. https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/

Greenberg, A. (n.d.). SECURITY ISN'T ENOUGH. SILICON VALLEY NEEDS "ABUSABILITY" TESTING. In *Wired*. https://www.wired.com/story/abusability-testing-ashkan-soltani/

Guadalupe-Diaz, X. L., & Jasinski, J. (2016). “I Wasn’t a Priority, I Wasn’t a Victim”: Challenges in Help Seeking for Transgender Survivors of Intimate Partner Violence. *Http://Dx.Doi.Org/10.1177/1077801216650288*, *23*(6), 772–792. https://doi.org/10.1177/1077801216650288

Guberek, T., McDonald, A., Simioni, S., Mhaidli, A. H., Toyama, K., & Schaub, F. (2018). Keeping a low profile? Technology, risk and privacy among undocumented immigrants. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3173574.3173688

Hackworth, L. (2018a). Limitations of “Just Gender”: The Need for an Intersectional Reframing of Online Harassment Discourse and Research. *Mediating Misogyny*, 51–70. https://doi.org/10.1007/978-3-319-72917-6_3

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. https://doi.org/10.1016/j.heliyon.2017.e00346

Hansen, L. (2000). The little mermaid’s silent security dilemma and the absence of gender in the Copenhagen School. *Millennium*. https://doi.org/10.1177/03058298000290020501

Haraway, D. (1988). Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. *Feminist Studies*. https://doi.org/10.2307/3178066

Harding, S. (2001). Feminist Standpoint Epistemology. *The Gender and Science Reader*.

Harding, S. (2016). Whose science? Whose knowledge?: Thinking from women’s lives. In *Whose Science? Whose Knowledge?: Thinking from Women’s Lives*. https://doi.org/10.2307/2186048

Harris, B. A., & Woodlock, D. (2019). Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies. *The British Journal of Criminology*, *59*, 530–550. https://doi.org/10.1093/BJC/AZY052

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019). Clinical computer security for victims of intimate partner violence. *Proceedings of the 28th USENIX Security Symposium*.

Hayes, G. R. (2011). The relationship of action research to human-computer interaction. *ACM Transactions on Computer-Human Interaction*. https://doi.org/10.1145/1993060.1993065

Heath, C. P. R., Hall, P. A., & Coles-Kemp, L. (2018). Holding on to dissensus: Participatory interactions in security design. *Strategic Design Research Journal*. https://doi.org/10.4013/sdrj.2018.112.03

Held, V. (2006). The Ethics of Care: Personal, Political, and Global. In *The Ethics of Care: Personal, Political, and Global*. https://doi.org/10.1093/0195180992.001.0001

Henry, N., & Flynn, A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support: *Https://Doi.Org/10.1177/1077801219863881*, *25*(16), 1932–1955. https://doi.org/10.1177/1077801219863881

Henry, N., Flynn, A., & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, *26*(15–16). https://doi.org/10.1177/1077801219875821

Hesse-Biber, S., Leavy, P., & Brooks, A. (2012). Feminist Standpoint Epistemology: Building Knowledge and Empowerment Through Women's Lived Experience. In *Feminist Research Practice*. https://doi.org/10.4135/9781412984270.n3

Hester, H. (2018). Care under capitalism: The crisis of "women's work." *IPPR Progressive Review*, *24*(4). https://doi.org/10.1111/newe.12074

Hochschild, A. R. (2015). Global care chains and emotional surplus value. In *Justice, Politics, and the Family*. https://doi.org/10.4324/9781315633794

Hooks, B. (1984). *Feminist Theory: From Margin to Center*. New York: Routledge.

Hooks, B. (1986). Sisterhood: Political Solidarity between Women. *Feminist Review*, *23*, 125. https://doi.org/10.2307/1394725

Hörschelmann, K., & Reich, E. (2017). Entangled (In)Securities: Sketching the Scope of Geosocial Approaches for Understanding "Webs of (In)Security"1. *Geopolitics*. https://doi.org/10.1080/14650045.2016.1214821

Hudson, H. (2016). 'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security. *Http://Dx.Doi.Org/10.1177/0967010605054642*, *36*(2), 155–174. https://doi.org/10.1177/0967010605054642

Hussain, H. (2021). *Trauma-informed design: understanding trauma and healing | by Hera Hussain | Chayn*. Chayn. https://blog.chayn.co/trauma-informed-design-understanding-trauma-and-healing-f289d281495c

Irani, L. (2018). “Design Thinking”: Defending Silicon Valley at the Apex of Global Labor Hierarchies. *Catalyst: Feminism, Theory, Technoscience*, *4*(1), 1–19. https://doi.org/10.28968/cftt.v4i1.29638

JCWI. (2020). *The Hostile Environment explained | Joint Council for the Welfare of Immigrants*. The Joint Council for the Welfare of Immigrants. https://www.jcwi.org.uk/the-hostile-environment-explained

Johnson, M., Lee, M., McCahill, M., & Mesina, M. R. (2020). Beyond the `All Seeing Eye’: Filipino Migrant Domestic Workers’ Contestation of Care and Control in Hong Kong. *Ethnos*, *85*. https://doi.org/10.1080/00141844.2018.1545794

Jones, L. M., & Mitchell, K. J. (2016). Online Harassment. In *The Wiley Handbook on the Psychology of Violence*. https://doi.org/10.1002/9781118303092.ch29

Jones, S. L., Muir, K., Collins, E. I. M., Joinson, A., & Levordashka, A. (2019). What is “cyber security”?: Differential language of cyber security across the lifespan. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290607.3312786

Jonsson, T. (2016). The narrative reproduction of white feminist racism. *Feminist Review*. https://doi.org/10.1057/fr.2016.2

Kaba, M. (2017). *Free Us All – The New Inquiry*. The New Inquiry. https://thenewinquiry.com/free-us-all/

Kadri, T. E. (2020). Networks of Empathy Networks of Empathy Repository Citation Repository Citation NETWORKS OF EMPATHY. *Utah L. Rev*, *1075*.

Kalayaan. (2019). *DIGNITY, NOT DESTITUTION: The impact of differential rights of work for migrant domestic workers referred to the National Referral Mechanism*. http://www.kalayaan.org.uk/wp-content/uploads/2019/10/Kalayaan_report_October2019.pdf

Kaldor, M. (2007). *Human Security* . Polity Press. https://books.google.co.uk/books?hl=en&lr=&id=gJsuLTflHecC&oi=fnd&pg=PR5&dq=human+security&ots=X1i2UUAoDR&sig=Uy5cIdsWy7U1k1C6G1Y2c8nazqk&redir_esc=y#v=onepage&q=human%20security&f=false

Kamara, S. (2020). *Crypto for the People, Invited talk at Crypto 2020 - YouTube*. https://www.youtube.com/watch?v=Ygq9ci0GFhA

Katell, M., Young, M., Dailey, D., Herman, B., Guetler, V., Tam, A., Binz, C., Raz, D., & Krafft, P. M. (2020). Toward situated interventions for algorithmic equity: Lessons from the field. *FAT**

2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3351095.3372874

Kazansky, B. (2021). 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*, *8*(1).

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Kemmis, S., McTaggart, R., & Nixon, R. (2014). The action research planner: Doing critical participatory action research. In *The Action Research Planner: Doing Critical Participatory Action Research*. https://doi.org/10.1007/978-981-4560-67-2

Kindon, S., Pain, R., & Kesby, M. (2007a). Participatory Action Research: Origins, approaches and methods. In *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*.

Kindon, S., Pain, R., & Kesby, M. (2007b). Participatory Action Research: Origins, approaches and methods. In *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*.

Kishimoto, K., & Mwangi, M. (2009). Critiquing the Rhetoric of "Safety" in Feminist Pedagogy: Women of Color Offering an Account of Ourselves. *Feminist Teacher*, *19*(2), 87–102. https://doi.org/10.1353/FTR.0.0044

Lara Guzmán, R., & Amrute, S. (2019). *How to Cite Like a Badass Tech Feminist Scholar of Color | by rigo | Data & Society: Points*. Data & Society: Points. https://points.datasociety.net/how-to-cite-like-a-badass-tech-feminist-scholar-of-color-ebc839a3619c

Law Society. (2022). *A guide to race and ethnicity terminology and language | The Law Society*. Law Society. https://www.lawsociety.org.uk/en/topics/ethnic-minority-lawyers/a-guide-to-race-and-ethnicity-terminology-and-language

Leitão, R. (2019a). Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. *ACM Conference on Designing Interactive Systems*, 527–539. https://dl.acm.org/citation.cfm?id=3322366

Levy, K. (2019). Intimate Surveillance. *Idaho Law Review*, *51*(3). https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/5

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1). https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222

Lewis, R., Sharp, E., Remnant, J., & Redpath, R. (2015). 'Safe Spaces': Experiences of Feminist Women-Only Space: *Https://Doi.Org/10.5153/Sro.3781*, *20*(4). https://doi.org/10.5153/SRO.3781

Limer, E. (2017). *Facebook's Nude Photo Scheme Is a Bad Version of a Good Idea*. Popular Mechanics. https://www.popularmechanics.com/technology/security/news/a28955/facebook-revenge-porn-abuse-prevention-image-hashing/

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How Abuse is Getting Smarter. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3350615

Lorde, A. (1984). The Master's Tools Will Never Dismantle the Master's House . In *Sister Outsider: Essays and Speeches* (pp. 110–114). Crossing Press .

Lorde, A. (1988). A Burst of Light. *Essence*, *18*(9).

Lucero, L. (2017). Safe spaces in online places: social media and LGBTQ youth. *Multicultural Education Review*. https://doi.org/10.1080/2005615X.2017.1313482

Macgillivray, A., & Wong, N. (2020). *Origins of Trust and Safety*. Data & Society. https://datasociety.net/library/origins-of-trust-and-safety/

Mackenzie, D., & Wajcman, J. (1999). *The social shaping of technology* (2nd ed.). Open University Press. http://eprints.lse.ac.uk

Madden, M., Gilman, M. E., Levy, K., & Marwick, A. E. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930247

Mahar, K., Zhang, A. X., & Karger, D. (2018). Squadbox: A tool to combat email harassment using friendsourced moderation. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3173574.3174160

McDonald, N., Badillo-Urquiola, K., Ames, M. G., Dell, N., Keneski, E., Sleeper, M., & Wisniewski, P. J. (2020). Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3334480.3375174

McKenna, S., Staheli, D., & Meyer, M. (2015). Unlocking user-centered design methods for building cyber security visualizations. *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015*. https://doi.org/10.1109/VIZSEC.2015.7312771

McMahon, C. (2020). In Defence of the Human Factor. *Frontiers in Psychology*, *11*(1390).

Morozov, E. (2013). To Save Everything Click Here. *Scientific American*.

Murray, C. E., Evette Horton, G., Higgins Johnson, C., Notestine, L., Garr, B., Marsh Pow, A., Flasch, P., & Doom Murray, E. (2015). Domestic Violence Service Providers' Perceptions of Safety Planning: a Focus Group Study. *Journal of Family Violence*, *30*, 381–392. https://doi.org/10.1007/s10896

NCSC. (2020). *Decrypting diversity: Diversity and inclusion in cyber security*.

Neocleous, M. (2003). Critique of security. In *Critique of Security*. https://doi.org/10.3366/edinburgh/9780748633289.001.0001

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-005-4582-3

No Tech for Tyrants. (2022). *Surveillance Tech Perpetuates Police Abuse of Power*. https://notechfortyrants.org/2022/11/07/new-report-surveillance-tech-perpetuates-police-abuse-of-power/

Noble, S. U. (2018a). Algorithms of oppression: How search engines reinforce racism. In *NYU Press*. https://doi.org/10.15713/ins.mmj.3

Noble, S. U. (2018b). Algorithms of oppression: How search engines reinforce racism. In *NYU Press*. https://doi.org/10.15713/ins.mmj.3

Nuttall, L., Evans, J., Franklin, M., & James, S. B. (2019). *Coercive Control Resistant Design* (pp. 1–24).

Office, H. (2021). *Domestic workers who are victims of modern slavery - caseworker guidance*.

Oldenziel, R. (1999). Making Technology Masculine : Men, Women, and Modern Machines in America, 1870-1945. In *Making Technology Masculine : Men, Women, and Modern Machines in America, 1870-1945*. https://doi.org/10.5117/9789053563816

on Drugs, U. N. O., & Crime. (2018). *GLOBAL STUDY ON HOMICIDE Gender-related killing of women and girls* (pp. 1–64).

Owens, K., Roesner, F., Kohno, T., Alem, A., & Roesner, F. (2022). Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, {Human-Centered}, and Legal Perspectives. *31st USENIX Security Symposium (USENIX Security 22)*, 4077–4094. https://www.usenix.org/conference/usenixsecurity22/presentation/zhang-zenong

Oyěwùmí, O. (1997). *The invention of women : making an African sense of Western gender discourses*. 229. https://www.upress.umn.edu/book-division/books/the-invention-of-women

Pain, R., Whitman, G., & Milledge, D. (2010). *Participatory ActionResearch Toolkit:An Introduction to Using PAR as an Approachto Learning , Research and Action*.

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019a). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *ACM International Conference Proceeding Series*, 1–15. https://doi.org/10.1145/3368860.3368861

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019b). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *ACM International Conference Proceeding Series*, 1–15. https://doi.org/10.1145/3368860.3368861

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019c). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *ACM International Conference Proceeding Series*, 1–15. https://doi.org/10.1145/3368860.3368861

PenzeyMoog, E. (2021). *Design for Safety*. A Book Apart.

Perez, C. C. (2019). *Invisible Women*. Penguin Books.

Petty, T. (2019). *Safety vs. Security: Are You Safe or Are You Secure?* Our Data Bodies. https://www.odbproject.org/2019/01/18/safety-vs-security-are-you-safe-or-are-you-secure/

Pierce, J., Fox, S., Merrill, N., & Wong, R. (2018). Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 139:1-139:24. https://doi.org/10.1145/3274408

Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists - Hacking//Hustling. (n.d.). Retrieved February 24, 2022, from https://hackinghustling.org/posting-into-the-void-content-moderation/

Potts, A., Kolli, H., & Fattal, L. (2022). Whose voices matter? Using participatory, feminist and anthropological approaches to centre power and positionality in research on gender-based violence in emergencies. *Https://Doi.Org/10.1080/17441692.2022.2062026*. https://doi.org/10.1080/17441692.2022.2062026

Powney, D., & Graham-Kevan, N. (2019). Male Victims of Intimate Partner Violence: A Challenge to the Gendered Paradigm. *The Palgrave Handbook of Male Psychology and Mental Health*, 123–143. https://doi.org/10.1007/978-3-030-04384-1_7

Qureshi, A., Morris, M., & Mort, L. (2020). Access denied: The human impact of the hostile environment | IPPR. *IPPR: The Progressive Policy Think Tank*, *60*(4), 76–87. https://doi.org/10.1177/0306396819825788

Ramokapane, K. M., Rashid, A., & Such, J. M. (2019). "I feel stupid I can't delete...": A study of users' cloud deletion practices and coping strategies. *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017*.

Reyes Cruz, M. (2008). What If I Just Cite Graciela? Working Toward Decolonizing Knowledge Through a Critical Ethnography: *Http://Dx.Doi.Org/10.1177/1077800408314346*, *14*(4), 651–658. https://doi.org/10.1177/1077800408314346

Robinson, F. (2011). The ethics of care: A feminist approach to human security. In *The Ethics of Care: A Feminist Approach to Human Security*. https://doi.org/10.5860/choice.49-5933

Roe, P. (2008). The 'value' of positive security. *Review of International Studies*, *34*(4), 777–794. https://doi.org/10.1017/S0260210508008279

Sambasivan, N., Matthews, T., Batool, A., Thomas, K., Ahmed, N., Gaytán-Lugo, L. S., Nemer, D., Bursztein, E., Churchill, E., & Consolvo, S. (2019). "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300232

Schwartz, B., & Neff, G. (2019). The gendered affordances of Craigslist "new-in-town girls wanted" ads. *New Media and Society*. https://doi.org/10.1177/1461444819849897

Sedacca, N. (2019). Migrant domestic workers and the right to a private and family life. *Netherlands Quarterly of Human Rights*, *37*. https://doi.org/10.1177/0924051919884754

Sedacca, N. (2022). Domestic Workers, the 'Family Worker' Exemption from Minimum Wage, and Gendered Devaluation of Women's Work. *Industrial Law Journal*. https://doi.org/10.1093/INDLAW/DWAC005

Sharp, A. (n.d.). *Comment: victims of slavery are trapped in destitution by right to work restrictions - Free Movement*. Free Movement. Retrieved November 30, 2021, from https://www.freemovement.org.uk/national-referral-mechanism-right-to-work-restrictions/

Shepherd, L. J., & Weldes, J. (2008). Security: The State (of) Being Free From Danger? *Globalization and Environmental Challenges*, 529–536. https://doi.org/10.1007/978-3-540-75977-5_39

Shostack, A. (2014a). *Threat Modeling: Designing for Security*. Wiley.

Shostack, A. (2014b). *Threat Modeling: Designing for Security*. Wiley.

Sim, K. (n.d.). *Victim blaming meets technological objectivity: Anti-rape technology and its design*. XYZ Information Activism. Retrieved March 10, 2022, from https://xyz.informationactivism.org/en/victim-blaming-meets-technology/

Sim, K., & Zevenbergen, B. (2017). *Design Ethics for Gender-Based Violence and Safety Technologies*. Freedom to Tinker . https://freedom-to-tinker.com/2017/07/24/design-ethics-for-gender-based-violence-and-safety-technologies/

Simko, L., Lerner, A., Ibtasam, S., Roesner, F., & Kohno, T. (2018). Computer Security and Privacy for Refugees in the United States. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*. https://doi.org/10.1109/SP.2018.00023

Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St Antony's International Review*, 83–100.

Slupska, J., Dawson Duckworth, S. D., Ma, L., & Neff, G. (2021). Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411763.3451731

Slupska, J., & Lindsay Brown, M. (2021). Aiding Intimate Violence Survivors in Lockdown: Lessons about Digital Security in the COVID-19 Pandemic. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3897863

Slupska, J., & Tanczer, L. (n.d.). Intimate Partner Violence (IPV) Threat Modeling: Tech abuse as cybersecurity challenge in the Internet of Things (IoT). In *Technology-Facilitated Violence and Abuse – International Perspectives and Experiences*. Emerald Publishing.

Slupska, Toby Shulruff, & Tara Hairston. (2021). *Cybersecurity must learn from and support advocates tackling online gender-based violence | UNIDIR*. United Nations Institute of Disarmament Research. https://unidir.org/commentary/cybersecurity-online-GBV

Smith, E. (2017). *Did Facebook finally figure out that consent is more important than nipples? | Take Back The Tech*. Take Back Tech . https://takebackthetech.net/blog/did-facebook-finally-figure-out-consent-more-important-nipples

Smith, G. M. (2005). Into Cerberus' Lair: Bringing the Idea of Security to Light1. *Http://Dx.Doi.Org/10.1111/j.1467-856x.2005.00204.x*, *7*(4), 485–507. https://doi.org/10.1111/J.1467-856X.2005.00204.X

Smith, L., Rosenzweig, L., & Schmidt, M. (2010). Best Practices in the Reporting of Participatory Action Research: Embracing Both the Forest and the Trees 1Ψ7: *Http://Dx.Doi.Org/10.1177/0011000010376416*, *38*(8), 1115–1138. https://doi.org/10.1177/0011000010376416

Smith, P., & Mackintosh, M. (2007). Profession, market and class: nurse migration and the remaking of division and disadvantage. *Journal of Clinical Nursing*, *16*(12), 2213–2220. https://doi.org/10.1111/J.1365-2702.2007.01984.X

Sokoloff, N. J., & Dupont, I. (2005). Domestic Violence at the Intersections of Race, Class, and Gender. *Violence Against Women*. https://doi.org/10.1177/1077801204271476

Solms, R. von, & Niekerk, J. van. (2013). From information security to cyber security. *Computers and Security*. https://doi.org/10.1016/j.cose.2013.04.004

Srinivasan, A. (2021). Amia Srinivasan: the politics of safety . *Financial Times*. https://www.ft.com/content/de097d02-3fa9-4041-ade2-d517af30818c?sharetype=blocked

Srinivasan, A. (2022). *The Right to Sex*. Bloomsbury Publishing PLC.

Stahl, B. C., Doherty, N. F., Shaw, M., & Janicke, H. (2014). Critical Theory as an Approach to the Ethics of Information Security. *Science and Engineering Ethics*, *20*(3). https://doi.org/10.1007/s11948-013-9496-6

Stark, E. (n.d.). *Coercive control: How men entrap women in personal life. - PsycNET*. Oxford University Press. Retrieved October 7, 2021, from https://psycnet.apa.org/record/2007-05264-000

Stark, E., & Hester, M. (2018). Coercive Control: Update and Review: *Violence Against Women*, *25*(1), 81–104. https://doi.org/10.1177/1077801218816191

Stark, L. (2016). The emotional context of information privacy. *Information Society*. https://doi.org/10.1080/01972243.2015.1107167

Statt, N. (2018). *Facebook is expanding its unconventional approach to combating revenge porn - The Verge*. The Verge. https://www.theverge.com/2018/5/23/17386972/facebook-revenge-porn-combat-uploading-hashing-nude-photos

Strohmayer, A. (2020). *Sewing Through The Pandemic – Trips and Flips*. http://tripsandflips.com/sewing-through-the-pandemic/

Strohmayer, A., Bellini, R., & Slupska, J. (2022). Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. *IEEE Pervasive Computing*, 1–9. https://doi.org/10.1109/MPRV.2022.3182222

Strohmayer, A., Clamen, J., & Laing, M. (2019). *Technologies for Social Justice*. https://doi.org/10.1145/3290605.3300882

Strohmayer, A., Slupska, J., Bellini, R., Neff, G., Coventry, L., Hairston, T., & Dodge, A. (2021). *TRUST AND ABUSABILITYTOOLKIT: Centering Safety in Human-Data Interactions*.

Suchman, L. (n.d.). *Agencies in Technology Design: Feminist Reconfigurations*.

Suk, J. (2011). At Home in the Law: How the Domestic Violence Revolution Is Transforming Privacy. In *Yale University Press*.

Sultana, S., Deb, M., Ananya, B., Alam, S. M. R., Hasan, S., Chakraborty, T., Roy, P., Ahmed, S. F., Moitra, A., Amin, M. A., Islam, A. K. M. N., & Ahmed, S. I. (2021). Unmochon': A tool to combat online sexual harassment over facebook messenger. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445154

Tanczer, L. M., López-Neira, I., & Parkin, S. (2021a). 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence*. https://doi.org/10.1332/239868021X16290304343529

Tanczer, L. M., López-Neira, I., & Parkin, S. (2021b). 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence*, *5*(3), 431–450. https://doi.org/10.1332/239868021X16290304343529

TechvsAbuse. (2019). *Tech vs Abuse: Design Challenges*. https://www.techvsabuse.info/design-challenges

Tereshkin, A. (2010). Evil maid goes after PGP whole disk encryption. *SIN '10: Proceedings of the 3rd International Conference on Security of Information and Networks*, 2. https://doi.org/10.1145/1854099.1854103

The nature and impact of domestic abuse. (2018). In *Women's Aid*.

Tickner, J. A. (1993). Gender in International Relations: Feminist Perspectives on Achieving Global Security. *Political Science Quarterly*. https://doi.org/10.2307/2152026

Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review*. https://doi.org/10.1080/1040265042000210148

Trans & Women's Action Camp. (n.d.). *Anti-Oppression & Safer Space Policies – welcome to "twac". scroll down!* Retrieved February 16, 2022, from https://twac.wordpress.com/ao/

Tronto, J. (1995). Moral Boundaries: A Political Argument for an Ethic of Care. In *International Philosophical Quarterly*.

True, J. (2012). Securitizing Feminism or Feminist Security Studies? *International Studies Review*, *14*(1), 193–195. https://doi.org/10.1111/J.1468-2486.2012.01083.X

Tseng, E., Bellini, R., McDonald, N., Danos, M., Greenstadt, R., McCoy, D., Dell, N., & Ristenpart, T. (2020). The Tools and Tactics Used in Intimate Partner Surveillance:An Analysis of Online Infidelity Forums. *ArXiv Preprint ArXiv:2005.14341*. https://arxiv.org/abs/2005.14341

Tseng, E., Freed, D., Engel, K., Ristenpart, T., & Dell, N. (2021). A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. *CHI Conference on Human Factors in Computing Systems (CHI '21)*.

UK, G. (2020). *The Ripple Effect: Covid-19 and the Epidemic of Online Abuse*. https://fixtheglitch.org/covid19/

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1–22. https://doi.org/10.14763/2020.4.1533

Vera-Gray, F. (2018). The right amount of panic: How women trade freedom for safety. In *The Right Amount of Panic: How women trade freedom for safety*.

Vera-Gray, F. (2020). The whole place self : reflecting on the original working practices of rape crisis. *Journal of Gender-Based Violence, 2020, Vol.4(1), Pp.59-72 [Peer Reviewed Journal]*, *4*(1), 59–72. https://doi.org/10.1332/239868019X15682997635986

Vera-Gray, F., & Kelly, L. (2020). Contested gendered space: public sexual harassment and women's safety work. *International Journal of Comparative and Applied Criminal Justice*, *44*(4). https://doi.org/10.1080/01924036.2020.1732435

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*. https://doi.org/10.1016/j.cose.2013.04.004

Wajcman, J. (2009). Feminist theories of technology. *Cambridge Journal of Economics*. https://doi.org/10.1093/cje/ben057

Wang, Y. (2018). Inclusive security and privacy. *IEEE Security and Privacy*, *16*(4). https://doi.org/10.1109/MSP.2018.3111237

Warford, N., Matthews, T., Yang, K., Akgul, O., Consolvo, S., Gage Kelley, P., Malkin, N., Mazurek, M. L., Sleeper, M., & Thomas, K. (2022). SoK: A Framework for Unifying At-Risk User Research. *2022 IEEE Symposium on Security and Privacy (SP)*. https://dblp.uni-trier.de/search

Webber, F. (2019). On the creation of the UK's 'hostile environment.' In *Race and Class* (Vol. 60, Issue 4). https://doi.org/10.1177/0306396819825788

Whittaker, M. (2021). The steep cost of capture. *ACM Interactions*. https://interactions.acm.org/archive/view/november-december-2021/the-steep-cost-of-capture

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *8th USENIX Security Symposium*.

Williams Institute. (n.d.). Transgender people over four times more likely than cisgender people to be victims of violent crime. Retrieved March 14, 2022, from https://williamsinstitute.law.ucla.edu/press/ncvs-trans-press-release/

Wilton Park. (2022). *Building a shared agenda on the evidence base for Gender-Based Online Harassment and Abuse - Wilton Park*. https://www.wiltonpark.org.uk/event/building-a-shared-agenda-on-the-evidence-base-for-gender-based-online-harassment-and-abuse/

Wittes, B. (2016). Sextortion as Cybersecurity: Defining Cyber Risk Too Narrowly. In *Lawfare*.

Wolfson, T., Huws, U. E., Farrar, J. M., & Aslam, Y. (2022). 'Alongside but not in front': Reflections on engagement, disengagement and ethics in action research with workers. *Work Organisation, Labour & Globalisation*.

Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*. https://doi.org/10.1177/1077801216646277

Wuyts, K., Scandariato, R., & Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modelling methodology. *Journal of Systems and Software*, *96*, 122–138. https://doi.org/10.1016/J.JSS.2014.05.075

Wyatt, S. (2008a). Technological Determinism is Dead; Long Live Technological Determinism. In E. J. ; Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The Handbook of Science and Technology Studies* (pp. 165–180). MIT Press. https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wyatt-2007b.pdf#page=181

Wyatt, S. (2008b). The Handbook of Science and Technology Studies. In E. J. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The Handbook of Science and Technology Studies*. MIT Press.

Xiong, W., & Lagerström, R. (2019). Threat modelling – A systematic literature review. In *Computers and Security*. https://doi.org/10.1016/j.cose.2019.03.010

Yao, Y., Basdeo, J. R., Kaushik, S., & Wang, Y. (2019). Defending my castle: A co-design study of privacy mechanisms for smart homes. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300428

Ye, M., Jiang, N., Yang, H., & Yan, Q. (2017). Security analysis of Internet-of-Things: A case study of August smart lock. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. https://doi.org/10.1109/INFCOMW.2017.8116427

Yeo, C. (2017). *The hostile environment: what is it and who does it affect? | New Europeans*. NewEuropeans.Net. https://neweuropeans.net/article/1927/hostile-environment-what-it-and-who-does-it-affect

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

Zeng, E., Mare, S., Roesner, F., Clara, S., Zeng, E., Mare, S., & Roesner, F. (2017). End User Security and Privacy Concerns with Smart Homes T. *Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, *Soups*.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*. https://doi.org/10.1016/j.ijhcs.2019.05.005

APPENDICES

Appendix 1.1: Reconfigure Participant Agreement

Reconfigure: Digital Privacy Workshop

Participant Agreement

Please initial in the boxes below.

- ☐ I have read and understood the information about this project and have had the opportunity to ask questions and get satisfactory answers.
- ☐ I understand that agreeing to take part means that the following data may be used for an ongoing research project (*please check each):*
  - ☐ Survey responses: I understand that any answers I input to the Mentimeter online form may be used as research data
  - ☐ Audio recordings: I understand that I might be asked to participate in a recorded focus group or interview and that I can refuse this request
  - ☐ Field notes: I understand that researchers may take field notes
  - ☐ Photos: I understand that I may be asked to be photographed and that I can refuse this request. Photos being taken throughout the event may be included alongside research findings, which could lead to me to be identified and linked with general findings of the workshop (but not individual responses).
- ☐ I understand that my participation is voluntary, and that I can choose not to participate in part or all of the project. I can withdraw at any stage simply by informing the research of my decision before end of May 2020 (project end date) without being penalized or disadvantaged in any way
- ☐ I understand that any information I provide is confidential, and that no responses that could identify me will be disclosed in any reports on the project, or to any other party. No identifiable personal data (other than photos) will be published and the data will not be shared with any other organization.
- ☐ I am aware of whom to contact should I have questions following my participation.
- ☐ I understand that this project has been reviewed by and received ethics clearance through the Central University Research Ethics Committee at the University of Oxford (reference number: SSH_OII_CIA_20_004).

By signing, I agree to participate in this study.

Name:……..*(please print)*

Signature:……

Date: .....

Appendix 1.1: Recruitment Material

Appendix 1.3: Reconfigure Example Schedule

Reconfigure: Digital Privacy Workshop

Schedule

6.35 – 6.45 Intro: workshop inspiration & aims, setting ground rules

The following questions will be displayed on Mentimeter, an interactive survey software. Participants will be warned that answers they enter through this program will be included in the research and displayed publicly during the workshop. A follow up email will include the questions in a survey format in case participants want to submit something privately or have new thoughts after the workshop.

Part 1: Introductions (6.45 – 7.00)

Participants asked to turn to person next to themselves & introduce themselves, then discuss question on screen (and submit answers if they are comfortable):

1. Why did you come to workshop today? What would you like to learn?
2. How much digital privacy/cybersecurity knowledge do you have?
3. Which gender do you identify as?
4. How old are you?

Part II: Threat modelling (7.00 – 7.30)

Separate out into groups of 3-5, guided by tech support

1. Which parts of your online life is it most important to you to protect?
2. What makes you feel threatened online? Can you remember a specific time you felt unsafe?
3. Which parts of your digital security would you like to improve?

Part III: Cybersecurity support session (7.30 – 8.20)

Stay in groups

- Primary: DIY Guide to Feminist Cybersecurity
- Secondary: EFF's Surveillance Self-Defense Kit, Tactical Tech Collective's Holistic Cybersecurity Manual

8.20 – 8.30 Break

Part IV: Discussion (8.30 – 9.10)

Stay in groups

1. How does cybersecurity make you feel?
2. How do personal experiences (such as gender, race, class, educational background, anything else) shape your engagement with cybersecurity?

3. Are there any cybersecurity tools that you haven't encountered yet but that you wish existed?
4. Should "good cybersecurity citizens" keep up to date with cybersecurity practices (such as those in the DIY Guide)? Is this an unfair burden? What is the alternative?

9.10 – 9.30 Pizza

Question left up: After this workshop, do you feel more empowered to engage with cybersecurity, or less so? If the latter, what do you think is missing? Be honest!

Appendix 2.1: Networks of Care List of Participants

Participants and their organisations are listed in Table \ref{table:bello}. As we are promoting advocates as experts in their field, we wanted to give advocates the chance to be identified by their name and organisation should they choose to do so \cite{Cruz2008}. Consequently, although participants in the study are pseudonymous by default, participants could also opt-in to use their real name. Asterisks (*) indicate areas where participants chose to use a pseudonym or keep details confidential.

Name	Organisation	Role	Focus	Country
Natalie Dolci[27]	Safe Campus and Technology-Enabled Coercive Control Initiative	Senior Violence Prevention and Response Specialist	Campus violence prevention and tech enabled coercive control	USA
Stephanie*	*	*	Domestic violence	*
Toby Shulruff	*	*	Domestic violence	USA
Sarah	*	*	Family violence	*
Luiza*	*	*	Women's services	*
Spike Curtis	Technology-Enabled Coercive Control Initiative	Volunteer technologist	Technology-enabled abuse	USA
Adam Dodge	End Technology-Enabled Abuse	CEO	Technology-enabled abuse	USA
Chris Warner	End Technology-Enabled Abuse	CEO	Technology-enabled abuse	USA
Susan Hickey	Harris County Domestic Violence Coordinating Counci	Advocacy Specialist	Domestic violence	USA
Rayme Lacey	Heart of Grant County	Advocate	Domestic violence	USA
Matthew*	*	Advocate	Domestic violence	*
Ben Walker	New Beginnings	Volunteer technologist	Tech enabled coercive control clinic	USA
Rebecca*	*	*	Sexual violence	*

[27] This interview draws on findings from a participatory action research project with Dana Cuomo in collaboration with the Technology-Enabled Coercive Control Initiative (Cuomo & Dolci, 2019a).

Anastasia*	*	*	Domestic and sexual violence	*
Amy Jacques	*	*	Domestic violence	*
Metzli Mejia	LA LGBT Center	Legal client advocate	LGBT+ rights	USA
Hera Hussein	Chayn	Founder and CEO	Gender-based violence	Global
Eva Galperin	Electronic Frontier Foundation	Director of Cybersecurity	Digital privacy & civil rights	USA
Bridgette Alexander	*	Domestic violence education specialist	Domestic violence	USA
Seabata Makoae	She-Hive Association and MenEngage Network Lesotho	Social worker and coordinator	Gender activism	Lesotho
Milcah*	*	Attorney	*	South Africa
Andrijana Radoicic Nedeljkovic	Atina	Advocate	Gender-based violence	Serbia
Emma Pickering	Refuge	Tech abuse team manager	Domestic violence	United Kingdom
Sol*	*	*	*	*
Farah Sattar	DCRYPTD	Founder and Security Researcher	Digital security	USA
Kate Worthington	Revenge Porn Helpline	Senior Helpline Practitioner	Intimate image abuse	UK

Appendix 2.2: Networks of Care Interview Protocol

1. Can you describe your role?
2. How did you first become involved in addressing the problem of technology-facilitated abuse (or 'tech abuse'?)
3. What kinds of tech abuse do you see most frequently?
4. How do you support survivors to address tech abuse?
5. Can you walk me through a case that you thought was particularly important or interesting?
6. (If psychological security has not come up) How do you address psychological distress which arise as a result of tech abuse in your work?
    - Alt: When doing safety planning for tech abuse, how do you balance digital security (i.e. protecting from account compromise, recommending security practices) with psychological well-being (i.e. not introducing unnecessary distress/ paranoia around devices, risk of retraumatization)?
    - Alt: if 'trauma' comes up – How do trauma-informed care practices affect how you give digital security advice?
7. What challenges do you face in supporting survivors?
8. Are there any demographic factors (like gender, race or immigration status) particular to the victims you support that shape their experience of tech abuse?
    - Patterns among perpetrators?
9. What kinds of mistakes can advocates make when supporting survivors of tech abuse?
10. Did you receive any formal training in supporting victim-survivors of tech abuse?
11. How does providing this support affect you?
12. What problems have you identified in the design of these technologies?
    - Alt: What would you want to say to companies that produce and sell digital technologies?
13. What are your preferred pronouns?
14. Is there anything else I should know about? Anything else you wanted to tell me?

Appendix 2.3: Networks of Care Recruitment Call

Call for participants: practitioners in domestic violence or information security who have supported survivors of technology-facilitated abuse (tech abuse)

I am conducting a study on how professionals support survivors of technology-facilitated abuse, including, stalking, harassment, surveillance or image-based abuse (or 'revenge porn' within intimate relationships (such as current or former romantic partners, family, friends or colleagues). Participating in this study will involve one one-hour long interview. The results will contribute to the doctoral thesis of the researcher, Julia Slupska, at the Oxford Internet Institute at the University of Oxford.

The criteria for participating in this study is to have supported at least three victim-survivors experiencing tech abuse either as a privacy advocate or a support worker in domestic or intimate partner violence.

Aims: By gaining a better understanding of how practitioners support victim-survivors, I hope to raise awareness of the critical work they do and highlight their expertise in this area. I also aim to identify best practices and understand where further research or support is needed. Lastly, this research will inform the development of an 'abusability toolkit' aimed to encourage digital technology designers to consider and account for how their products could be co-opted for abuse.

If you are interested in participating, please contact Julia Slupska at Julia.slupska@cybersecurity.ox.ac.uk. Please feel free to pass on this call to anyone who meets the criteria.