"They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers

Julia Słupska and Selina Cho, *University of Oxford;* Marissa Begonia, *Voice of Domestic Workers;* Ruba Abu-Salma, *King's College London;* Nayanatara Prakash, *University of Oxford;* Mallika Balakrishnan, *Migrants Organise*

https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-vulnerability

This paper is included in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

"They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers

Julia Słupska
University of Oxford

Selina Cho
University of Oxford

Marissa Begonia
Voice of Domestic Workers

Ruba Abu-Salma
King's College London

Nayanatara Prakash
University of Oxford

Mallika Balakrishnan
Migrants Organise

Abstract

The needs of marginalised groups like migrant domestic workers (MDWs) are often ignored in digital privacy and security research. If considered, MDWs are treated as 'bystanders' or even as threats rather than as targets of surveillance and legitimate security subjects in their own right. Using participatory threat modelling (PTM) as a method of incorporating marginalised populations' experiences, we designed and conducted five workshops with MDWs (n=32) in the UK to identify threats to their privacy and security. We found that MDWs named government surveillance, scams and harassment, and employer monitoring (in this order) as the primary threats to their privacy and security. We also examined the methods MDWs used to stay safe online, such as configuring the privacy settings of their online accounts and creating on- and offline community support networks. Based on our findings, we developed and disseminated a digital privacy and security guide with links to further resources that MDWs can refer to. We conclude by arguing that security research must consider broader social structures like gendered work and racialised border policy that foster insecurity in the lives of MDWs. We also present the key lessons of our work, including considering data sharing from the perspective of stakeholders who do not own technology devices but are affected by them, and reflecting on how security research can stop enabling harmful forms of surveillance.

1 Introduction

Migrant domestic workers (MDWs) work in private households, usually as cleaners or nannies, and have moved from their countries of origin. The International Labour Organisation (ILO) estimates that 17.2% of domestic workers globally are migrants, a percentage that is higher than other industries [43]. Domestic workers are mainly women, disproportionately from ethnic minorities, and/or migrants. 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 (e.g., [103]). As a result, they are often subject to isolated mistreatment in their workplaces [103], including but not limited to "humiliation, abuse, violence, exploitation and trafficking" [37].

MDWs experience a disproportionate amount of surveillance from both the government and their employers [103]. An increase in the use of smart home monitoring devices such as CCTV cameras has contributed to situations of pervasive monitoring. Yet, MDWs have hardly received any consideration in digital security research. Where domestic workers are discussed, they are often referred to as bystanders (e.g., [2, 15, 63, 81, 127]) or even as threats (e.g., [57, 102, 130]. Current discussions spanning privacy and data protection in smart homes often do not consider those who are vulnerable. Aggregate descriptions tend to obscure hidden populations such as MDWs, whose need for privacy may be critically associated with their livelihood and fundamental human rights. For example, the threat of surveillance and deportation due to data sharing may stop MDWs from reporting labour exploitation and/or sexual violence or from accessing key public services like healthcare [52].

Prior work has explored the needs, views, and privacy concerns of primary users (e.g., [8, 15, 16, 20, 41, 42, 49, 69, 70, 77, 78, 85]) and – to a lesser extent – bystanders (e.g., [14, 15, 96, 129]) with regard to IoT technologies and smart home devices, using mainly interviews and surveys. We extend this work on bystander privacy as well as work on how power imbalances shape privacy and security [52, 75, 103] using participatory threat modelling (PTM) [108]. PTM is a powerful technique that has not yet been utilised by the privacy and security community to study the experiences of marginalised populations like MDWs. PTM applies the principles of participatory security design [56] to threat modelling by inviting participants to identify and prioritise threats to their privacy and security. *Therefore, it is an open-ended process which does not focus on a specific type of device or context but rather centres participants' perspectives.*

Our study offers the first investigation into the threats posed to MDWs' privacy and security. Our research questions are:

RQ1. *What are MDWs' digital privacy and security concerns?* **RQ2.** *What are the technological means used to create insecurity amongst MDWs?* **RQ3.** *What do MDWs do to address those concerns?* **RQ4.** *How do MDWs understand online safety, privacy, and security?* **RQ5.** *What changes are necessary to create safe and just environments for MDWs?*

To answer these questions, we designed and conducted five workshops with MDWs (n=32) in the UK in partnership with Voice of Domestic Workers (VoDW)[1], a support group run by and for MDWs. In these workshops, we invited MDWs to define threats to their safety, privacy, and security. To avoid priming participants, we did not define these three concepts in advance. However, we used these terms as intertwined concepts in relation to the protection of personal information and other defences against threats, especially technology-mediated ones.

We identified three major categories of threats that impacted the sense of safety and security of our participants, which we present as part of the threat model perceived by MDWs: government surveillance, online scams and harassment, and employer monitoring (in this order) (RQ1). Surprisingly, unlike prior work on bystander privacy (see §2.1.1), where some groups of bystanders have viewed employer monitoring as the most serious threat, our MDW participants viewed immigration surveillance and online scams and harassment as more concerning threats. Even after securing their immigration status, some were concerned about exposing others who might be undocumented.

Our findings also revealed that online scams and harassment often targeted MDWs' characteristics (e.g., immigration status, gender), ultimately compounding and reinforcing threats, as well as exposing the "intersectional" set of challenges that MDWs already face as part of their identities [28, 93]. Participants had varying opinions of their employers' use of CCTV cameras for monitoring; some believed CCTV cameras protected them against false accusations, whereas others explained that cameras made them feel uncomfortable, nervous, or intimidated. These divided opinions partially explain why participants did not perceive employer monitoring as the most concerning threat.

The identified threats are intersecting and reinforcing, leading to significant harms, such as a pervasive sense of being watched as well as constant worry, isolation, and loneliness, compounding existing vulnerabilities; lack of trust in people and technology in general; and uncertainty about accessing public services funded by the government, such as the UK National Health Service (NHS), due to fear of data sharing with immigration enforcement (RQ2, RQ4). Although MDW participants did not clearly distinguish between safety, privacy, and security, they associated "*being safe*" with freedom from risk and harm and "*peace of mind*" (RQ4). We also examined methods such as configuring the privacy settings of online social accounts and creating on- and offline community support networks that participants employed to stay safe online and protect against different kinds of surveillance and monitoring (RQ3). Participants created meaningful sources of safety in community support organisations, enabling them to share experiences and knowledge to protect each other and organise for collective power.

The contributions of this paper are as follows:

- **Empirical.** This is the first in-depth investigation into the threats faced by MDWs in the field of digital privacy and security. Our empirical findings inform security researchers and legal institutions of the threats faced by MDWs and argue for the need to better protect MDWs. We identify legal and cultural changes, such as clearer laws on CCTV surveillance of workers in households, which are necessary to make MDWs safe (RQ5). We also offer technical design recommendations (e.g., nudging device owners towards ethical device use), and we reflect on how security research can stop enabling harmful forms of surveillance (RQ5).
- **Theoretical.** Our findings show how intersecting social structures like gender, race, and border controls produce privacy and security threats that could be faced by already marginalised populations. We argue security research must take these structural forces into account, to better defend against digital threats like surveillance and avoid reinforcing unjust power dynamics.
- **Pragmatic.** We provide a free digital privacy and security guide for MDWs (see §3.4), co-created with peer researchers in migrant support organisations, to make our findings accessible to the public and our participants' community. The guide serves as an educational platform for MDWs in the UK and other countries, to protect their on- and offline privacy and safety.
- **Methodological.** We adopt PTM to present novel perspectives of threats faced by a marginalised population that would not have been otherwise surfaced through other methodological approaches. The collaborative nature of our work, while acknowledging its ethical implications, provides a foundation for the technical community to conduct future research with marginalised groups.

2 Background and related work

2.1 Domestic workers' privacy and security

Digital security research tends to focus on companies, militaries, or (in the case of domestic products like IoT devices) owners of devices rather than groups like MDWs. When MDWs are included, they are represented as 'bystanders' or even as potential threats. In this section, we outline these representations and argue that domestic workers deserve protection as security subjects in their own right.

[1] https://www.thevoiceofdomesticworkers.com/

2.1.1 Bystanders and secondary users

Research on the security and privacy of multi-user smart homes mainly divides smart home residents into *primary users* and *secondary users* with varying levels of control over devices, as well as *bystanders* (those who do not control devices but are affected by them, such as domestic workers, co-habitants, visitors, and passers-by).

Many previous studies have mainly examined the views, privacy concerns, and choices of *primary users* with regard to IoT technologies (e.g., [1, 10, 14, 15, 25, 59, 60, 65, 122–124, 128, 132]). Further, several studies have explored how different factors (e.g., age, gender, health status, living situation, finances, technical background, power imbalances) affect primary users' perspectives, concerns, and choices within the context of using IoT technologies and – especially – smart home devices (e.g., [6, 8, 11, 15, 45, 49, 58, 69, 77, 78, 85, 95, 117]). For example, older adults [42] are more willing to accept monitoring by smart health devices – provided that surveillance enabled by these devices is key to healthcare – than younger adults (e.g., [70]).

Motivated in part by research on multi-user smart homes and shared housing (e.g., [25, 27, 31, 77, 78, 80, 94, 110, 132]), secondary users and bystanders have recently received more attention by the research community (e.g., [3,35,96,107,129]). This research suggests that some groups like domestic childcare workers are often uncomfortable working with smart home devices in their workplace, particularly if devices are seen as evidence of mistrust or lack of respect on the employer's part and/or are used to micromanage workers [14, 15].

2.1.2 Domestic workers as threats or security subjects

As bystanders, domestic workers are rarely considered in privacy and security threat models, which primarily focus on device owners. When considered, domestic workers are often presented as potential threats to the household, suggesting that temporary workers may, for example, return later to rob a house [130]. Perhaps the most egregious example of this is the scenario problematically described as the "evil maid attack", in which a hotel maid compromises an unattended device using, for example, a USB flash drive [102]. The unattended device owner is usually characterised as a company executive or a government official and the "evil maid" as an industrial spy in disguise [57]. Although "evil maid" attacks have been documented, the prevalence of this imagery and lack of analysis of the security threats domestic workers face point to a systematic defence of those who, like company executives or government officials, have wealth and power.

Bystander privacy research expands our understanding of which users are affected by technology, but the term 'bystander' risks implying that surveillance of domestic workers is accidental or unintentional. Surveillance can be pervasive and harmful to domestic workers [63] and is often the reason for purchasing surveillance devices, as is evident in the term "nanny cam". Thus, privacy and security researchers should view domestic workers not as accidental bystanders or potential threats but as people who deserve privacy and security in their own right. Otherwise, forms of marginalisation and power imbalances in the household will persist [82].

2.2 Power dynamics and imbalances

In this section, we outline the power imbalances that affect the lives of MDWs, particularly in the UK.

2.2.1 Power imbalances in the workplace

Technology can impact different groups of people differently (e.g., [32, 54, 76, 90, 113, 114]) by; e.g., negatively affecting their privacy and online safety [92] due to digital inequalities (e.g., [44, 135]). Even if people (in this case, domestic workers) have the skills needed to configure the privacy settings of a smart home device, they could be denied access to these settings and, thus, will not be able to control data collection and processing because data collectors (e.g., employers or smart home owners) are socially and economically powerful [7, 15, 18, 26, 33, 74, 79, 98, 99, 115]. Recently, Bernd et al. have conducted a user study with domestic workers in the US showing how power imbalances could lead to negative behavioural changes among workers [14]. Further, these imbalances could lead to discrimination [75] or domestic abuse [17, 40, 71, 73, 91, 100].

2.2.2 Surveillance of migrants

Security researchers have recently started studying how different groups of people face specific forms of marginalisation, such as undocumented migrants [53], refugees [105], sex workers [82, 111, 116], queer people [48], IPV survivors [39, 71], and activists [4]. This has led to calls for a recognition of "differential vulnerabilities" [93] 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" [119]. Marginalised people experience a disproportionate amount of surveillance; for example, those who rely on public benefits must share "personal information [...] far more routinely than wealthier citizens" [52, 75]. This is particularly true of migrants living under the UK's "hostile environment", a set of policies introduced in 2012 by the Home Office[2], with the aim of making 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 crime [38, 50]. The Home Office also has access to the data that public sector organisations use,

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

such as patient health data, details of migrant victims and witnesses of crimes, and reports of unsafe working conditions and exploitative employers [38]. These policies harm all migrants and racialised minorities [97, 121, 131], 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" [131].

2.2.3 MDWs at the intersection

MDWs are subject to 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 [103]. However, when MDWs work inside someone else's home, they have little recourse to protection from employer surveillance. Such surveillance practices can be harmful to both the employer and employee; e.g., ethnographic research on Filipino MDWs in Hong Kong has shown that digital surveillance in the home did not only result in MDWs evading control but also not delivering the best care [63].

MDWs mainly enter the UK with an Overseas Domestic Worker (ODW) visa [64, 88], allowing MDWs to accompany or join an employer based 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 do not have enough time to find another job before their visa expires. In exceptional cases, workers can extend their stay and work lawfully 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 [104]. Like other aspects of the hostile environment, these immigration policies by design make workers vulnerable to on- and offline threats.

2.2.4 Exploring solutions and interventions

This section discusses the solutions and interventions used in security research to help address the problems bystanders and similar groups of people face.

2.2.5 Technology design

Most product teams pay little attention to the user experience dimensions of privacy and security solutions [5, 12, 21–24, 134] or encounter challenges with deploying these solutions in the real world [13, 36, 86, 89, 101, 112]. As a result, current solutions have their own limitations [51, 66]. Yet, several methods have been proposed to protect the privacy of bystanders in multi-user smart homes by using signalling features [67], announcing and implementing data usage policies [68], or relying on contextual cues [9, 83, 87].

2.2.6 Participatory action research

Besides technical design recommendations, security researchers can support marginalised groups through directly providing technical support and advice. For example, tech-related abuse clinics [29, 39] use community-based participatory action research, in which researchers and practitioners work together to better understand a problem in cycles of action and reflection, to directly support survivors of technology-enabled IPV. The Reconfigure Network has also used participatory action research in the form of community-based workshops to help people address digital privacy and security needs, employing PTM [108].

PTM draws on participatory action research and participatory security design, a set of security methods used to avoid equating individual security with the security of a technical system [56]. As such, participants taking part in participatory security design studies can define threats to their own privacy and security, showing how "differential vulnerabilities" can be socially contingent on demographic factors [93]. Researchers have used participatory security design methods to investigate privacy mechanisms for smart home users [126] and IPV survivors [72].

Using such methods highlights why legal and social changes beyond technical fixes are needed to address privacy and security concerns. For example, research conducted as part of Reconfigure has supported changes in culture and legislation (e.g., holding technology companies accountable) instead of only developing new technical products [108].

3 Methods

This section outlines the methods we used for data collection (i.e., PTM workshops), data analysis, development of a digital privacy and security guide with VoDW (our partner organisation), and ethical considerations for and limitations of our study.

3.1 VoDW

We partnered with VoDW, a support group run by and for domestic workers in the UK. VoDW helps MDWs leave abusive and exploitative employers, supports its members with immigration issues, creates resources, and organises English language and IT classes. VoDW was interested in taking part in our study because it had noticed an increase in digital privacy and security concerns among its members, particularly during the COVID-19 pandemic. Our peer researcher at VoDW helped organise the workshops described below and

develop the questions we asked our participants. This was critical to ensure that our study and research would be useful to the MDW community.

3.2 PTM workshops

We designed and conducted five workshops (four for data collection and one for data analysis) with MDWs (n=32) in the UK. Each workshop had 5-7 participants. Using PTM, we asked participants to describe the threats they perceived to their privacy and security [108]. PTM is a method used to explore in depth the lived experiences of participants, especially those traditionally marginalised, regarding their privacy and security. Researchers using PTM invite participants to take part in workshops where participants whose experiences have been traditionally ignored collectively discuss what their privacy and security mean to them, model how they perceive threats to their own privacy and security, and explain the measures they would employ (or have employed) to protect themselves and improve their digital practices. PTM allows participants to feel a sense of community, such that they can share their thoughts in open and non-judgemental group discussions. We then asked about the methods and tools these MDWs employed to stay safe online and protect against social media surveillance. We encouraged all participants to ask any questions they had about staying safe online (we included answers to these questions in the digital privacy and security guide described below in §3.4). Participants' questions, as well as our (desk-based) research to answer these questions, were part of PTM (see Appendix A). Not all participants answered each question, as answering questions was on an opt-in basis. Thus, the number of participants represented in responses is not necessarily comprehensive.

Workshops were conducted online using Zoom. To protect participant anonymity, we did not take audio or video recordings. Instead, we used an online platform named Mentimeter[3], which allowed participants to anonymously submit answers to our questions, and a researcher took handwritten notes for audio discussions without including participants' names. We did not assign pseudonyms, keeping all data fully anonymous. The workshops were designed to collaboratively create knowledge with our participants; for example, if participants chose to anonymously share responses via Mentimeter, their responses were shown on a screen. This allowed participants to comment on and react to each one's contributions, creating a sense of communal sharing and debate. Participants were also allowed more than a single opportunity to recall their memories and ideas by exchanging their experiences. We continued organising and conducting workshops until we reached data saturation.

Participants had the choice not to answer any question and withdraw their contributions at any point in time. Measures like avoiding recording and communal sharing as well as the presence at each workshop of the VoDW researcher attempted to mitigate the significant power imbalances (both social and economic) which existed between the researcher and research participants, particularly in research with vulnerable populations [118]. Feminist methods generally attempt to centre participants' experiences and respect their agency; conducting research in a group setting in particular allows for a more egalitarian and less exploitative dynamic than other methods like interviews or large-scale surveys because participants are in a group of their peers throughout the research process and, therefore, can receive support and validation [84]. We note, however, that these measures only mitigated and did not fully equalise the power dynamics inherent in our research.

Participants were recruited through our project partner at VoDW and compensated £50 for a 1.5-hour workshop. Our participants were housecleaners and childcare workers. Before each workshop, we collected demographic information including gender, nationality, education level, and employment status. However, as VoDW was fairly small, we did not prioritise demographic factors in recruitment; the only inclusion criteria were being an MDW and over the age of 18. Furthermore, our demographic survey questions were optional to answer, so the results should be seen as indicative rather than comprehensive. 18 participants self-identified their nationality: 14 (44%) as Filipinos, 3 as British, and 1 as Indonesian. Out of 20 responses reporting gender, 16 participants self-identified as women, 3 preferred to self-describe, and 1 self-identified as non-binary. 1 had only completed primary school, 3 had completed secondary school up to 16 years, 5 had completed higher, secondary, or further education, and 8 had completed college or university.

3.3 Data analysis

We analysed our data using thematic analysis [19], which involved five stages: reading through the data (Mentimeter responses and focus group fieldnotes), developing a set of codes, collating these codes into themes, revising and consolidating themes, and then writing descriptions of themes. After developing initial themes, we conducted a data walkthrough workshop, as part of PTM, in which we invited some participants back to support us with data analysis.

At this fifth workshop (data walkthrough workshop), we presented our initial data analysis to participants, asking them to critique our interpretations. We presented initial findings from the workshops, allowing participants to push back on our interpretations verbally as well as through Mentimeter. In §4, we emphasised areas where participants pushed back on our interpretation. This process of participatory data interpretation allowed us to conduct research in a less hierarchical way, following feminist principles of participatory research [46].

[3] https://www.mentimeter.com/

3.4 Digital privacy and security guide

Based on the findings of our five participatory workshops with MDWs, we 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[4]. 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. In making the guide, we focused, where possible, on existing resources, such as the DIY Guide to Feminist Cybersecurity[5], the Citizens Advice online scams helper[6], and Kalayaan's Employment Rights webpage[7]. We made sure to include clear action points the reader could easily implement. We also focused on making the guide easily readable. Lastly, we avoided unnecessary intimidation or victim blaming. For example, we included reminders like "Avoiding surveillance by your employer should not have to be your responsibility. Employers need to understand and respect domestic workers' right to privacy and safety, and refrain from excessive monitoring". We are continuously soliciting feedback from our computer privacy and security as well as MDW communities on the guide, are incorporating feedback on a regular basis, and plan to organise workshops with MDWs to hear their input on the guide. We describe our guide structure in detail in Appendix B.

3.5 Ethics

Ethical considerations 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. In order to do this, we did not video or audio record workshops; we instead relied on handwritten notes which did not include participants' names, as well as used an online platform where participants could submit answers to our questions anonymously. Some participants also participated in our study outside their home and workplace; e.g., in a park, in order to avoid being overheard by employers. Further, 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 (as a result of recruitment by our peer researcher), all participants had right to remain 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 compensated each participant £50, 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.

3.6 Limitations

To protect participant anonymity and follow data minimisation principles, we did not record the workshops. Instead, we used handwritten notes and the Mentimeter platform for online responses to our questions. As a result, some information might have been lost. This was particularly the case, as all participants did not speak English as their first language, which led to the transcriber missing some of their comments and might have resulted in participants not understanding some questions. To mitigate this, the peer researcher co-facilitated each session and ensured to rephrase each question in multiple ways to aid understanding.

Although the collaboration of the peer researcher from VoDW was a great benefit to the project, her presence might have affected what participants felt comfortable expressing in the workshops. There was possibly an element of social desirability bias in the findings, as participants were likely to share ideas that they perceived as desirable to the researchers and their peers. To mitigate this, we used an online platform which allowed participants to submit answers *anonymously*.

Further, we did not follow up with participants to understand what impact the guide had on the MDW community. The guide we produced is in English, which means it may not be accessible to all MDWs. We are currently exploring the possibility of translating it into other common languages spoken by migrant communities in the UK.

Our work is limited by the size and diversity of our sample. We recruited participants from a single organisation, and over a third of the sample had the same nationality (Filipino). Further, we only focused on MDWs in the UK. While our sample does not fully represent all MDWs, the sensitive nature of the topic implies that participant access is a challenge on its own. As a first study with a focus on MDW online safety and privacy, and given we do not aim to generalise findings, our study surfaces insights which can be subsequently expanded upon with more focus on demographics.

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

[5] https://hackblossom.org/cybersecurity/

[6] https://www.citizensadvice.org.uk/consumer/scams/what-to-do-if-youve-been-scammed/

[7] http://www.kalayaan.org.uk/for-workers/employment-rights/

4 Findings

In our workshops, we invited participants to define their own threats to their safety, privacy, and security. Our findings are divided into three main parts: the threat model perceived by MDWs in §4.1 (RQ1, RQ2, RQ4), impact and harms experienced by MDWs in §4.2 (RQ2), and sources of safety in §4.3 (RQ3, RQ5). We do not use pseudonyms as we intentionally do not attribute statements to individuals in any way to ensure anonymity. We also include an indication of the frequency of specific findings, such as (2) or (3) for two or three repetitions of the same statement. However, the main purpose of qualitative research is not to generate generalisable quantitative results but to explore a phenomenon in depth.

4.1 Threat model perceived by MDWs

This section addresses RQ1, RQ2, and RQ4 by offering insights into how online safety, privacy, and security are perceived by MDWs, and how technologies surrounding their environments have been used to invoke a sense of insecurity.

When asking participants "*What are the main threats to your privacy, security, or safety?*", we did not define the terms 'privacy', 'security', or 'safety' in order to avoid priming participants, as we wanted to explore their own understandings of these often contested concepts. Instead, we asked "*What does being safe mean to you?*" Participants associated safety with being free from risk or harm (4); "*peace of mind*" (3); "*not worrying*" (2); limiting who can see personal information (3). Participants did not clearly distinguish between privacy, security, and safety when asked about these terms. We speculate this was the case because English is not the first language of most migrants, and these conceptual distinctions are particularly interesting to security professionals.

Based on participants' answers, we identified three main categories of threats to MDWs: government surveillance, online scams and harassment, and employer monitoring. 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 monitoring by employers [14] with whom they had the most interaction in their daily lives. However, participants considered government surveillance and online harassment to be more serious threats. Consequently, we followed this prioritisation in our own analysis.

4.1.1 Government surveillance

The first category of threats refers to government monitoring of MDWs to keep an eye on their immigration status. Participants reported that public bodies such as the Disclosure and Barring Service (DBS) or the 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 general practitioners. Three participants shared that they would like to learn about government tracking from establishments like the DBS or the 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 secured permanent 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 pandemic: "*[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.

4.1.2 Online scams and harassment

The second source of threat is online scams and harassment. Scams varied across different methods 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 they experienced 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?*" The majority of domestic workers are women [103] like our participants, 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 vulnerabilities, 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.

4.1.3 Employer monitoring

The third category of threats refers to how employers of domestic workers monitor their performance. Twenty workers reported they had worked in a home with a CCTV camera or a similar monitoring device, while 7 reported they had not. Participants' opinions were divided over employers' use of CCTV cameras for monitoring. Some participants argued these could be used to defend the house against intruders (4) or the workers themselves against false accusations (7), while others reported that cameras made them feel uncomfortable, nervous, or scared (12). One participant recalled their experience working with cameras: "*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 cameras would particularly be useful to an employer bullying their worker: "*[They can] slap and spit... [the] camera will know, [and we can] use it as [the] evidence.*"

Further, 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 it's 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 the 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 its inner workings.

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 could be used as proof against them especially in the case of family member exemptions (see [103] for a discussion of these legal loopholes, allowing employers to avoid minimum wage requirements): "*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 said: "*[An] employer can destroy [the data] unless the police gets there first*" or can enable access to the data, 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 it 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 views, 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, as well as allowed them to connect digitally. A combined lack of physical privacy and online privacy leads to a pervasive sense of being watched. These anecdotes 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 in which men 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.

4.2 Impact and harms

This section addresses RQ2 by exploring how the identified threats had an impact on participants, which was notable in technology-enabled mediums such as social media.

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 MDWs' everyday life and made it harder to form relationships in their new country (6).

The fear was particularly pronounced in online interactions: workers described mistrusting messages from strangers and even from family members, feeling that they might be subject to scams or identity theft (5). This was particularly

damaging given the centrality of technology and social media for contacting family abroad. Several workers described receiving help from their employers to figure out what an online scam was (3). One participant described changing her name on Facebook and hiding information about her workplace 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: "*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 about and low public trust in places of accessible support. The impact was harmful because participants 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. This made participants 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 workers live with someone else who may have a precarious immigration status, it obliges them to be conscious of not only their own safety but also that of others. Therefore, workers' understandings of safety and security were highly relational, as we describe in the next section.

Although the MDW 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.

4.3 Sources of safety

This section addresses RQ3 and RQ5 by describing the actions that MDWs had previously taken to address their concerns, as well as further necessary changes 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, participants often practiced regular care towards each other. Although VoDW is primarily concerned about providing immigration support and advice on visas, it 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 with my relatives [and] friends that in far country.*" This was particularly useful given the international background of the workers whose social networks might be located outside their resident country: "*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 about what to do if they became a victim of an online scam.

Knowledge is important to facilitate a sense of safety. Participants (8) reported the significance of being aware of CCTV camera locations and how that contributed to 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 camera footage in this way, this participant reported much more trust in her employer as a result. Some participants were even vocal about their rights to privacy and the need to draw a boundary where cameras 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). One participant said: "*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.*" This reflects the mobilised and politicised aspects of VoDW, which organises campaigns for legal and structural reform. It also shows 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 MDWs' working and private lives.

Although participants had a strong understanding of what kind of legal reform of immigration rules was needed, they were not certain about how laws governing technologies could protect them. For example, when we asked participants if they had questions for us, one asked: "*Is it legal to record workers in your home? Is it an invasion of privacy?*" To answer these questions, we realised that the UK law on CCTV camera recording in the home is both complex and ambiguous[8].

[8] We asked participants if they had any questions 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 questions and our research on UK data protection law to answer the questions.

CCTV camera installations in privately-owned homes are legal as long as CCTV cameras do not record those outside the property [61]. 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. It must be strictly targeted at gathering evidence linked to that activity, and cannot go beyond what is necessary for the investigation (ICO) [61]. In data protection laws, similar to employment laws, the right to privacy of a family is often used as an exemption from protection that workers need (ILO C189 [62]).

The most available sources of information online are websites for employers from nanny agencies[9] or surveillance equipment vendors[10] on "how to keep a legal eye on your babysitter". These have sometimes contradictory information which seems dubious.

Further, 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 results in inconsistent interpretation of one's status and rights, forming a root cause of constant insecurity. 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, in reality, may be complex and costly for 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.

5 Discussion

Based on our findings, we describe the study's lessons and takeaways in §5.1, as well as methodological and design implications of the research undertaken (including potential avenues for future research) in §5.2.

5.1 Key lessons and takeaways

5.1.1 Importance of intersectionality and power

We argue that domestic workers should not be blamed for the digital privacy and security threats we identified in this paper. Our findings highlight the need for the privacy and security literature to consider intersecting forms of marginalisation (due in part to different levels of social and economic power) (see

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

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

§2.2) and the broader social structures that create insecurity, and we echo calls to "discuss the value of intersectionality as a framework for understanding vulnerability to harms in security research" [48]. 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 [105].

Our participants' threat prioritisation (see §4.1) reflects the different impacts of surveillance on people with different social and legal statuses. Past research on domestic workers [15] has documented how the fear of losing jobs stopped workers from being able to negotiate CCTV camera use with employers. MDWs both share these concerns of precarious workers and have to 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 workers cannot find a new employer.

Particularly, we see a need to address the relationship between digital security and political phenomena, such as the hostile environment (see §2.2.2), 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 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 that the literature currently neglects.

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 [53] and queer people [48], which found that research on marginalised groups often results in recommendations for structural changes to best protect these groups of people. Thus, although we conclude this paper with a section on design implications (see §5.2.2), we also focus on legal reform and non-technical interventions (see §5.1.2).

Politically contextualised analysis also offers security researchers insights into broader questions about the conceptual tools we use and assumptions we make. For example, our findings show that security design and privacy laws favour homeowners as the relevant subjects in cases where domestic workers are "guests" or "bystanders" (see §4.3). What implications and insights might result from disrupting this norm? Or, as another example, we noted that our participants often described both vulnerability and security in social/communal forms (see §4.3); 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 experiences of these concepts.

5.1.2 Legal and structural reform is necessary for safety

Our participants were clear that legal reform was a necessary change they needed to be safe online. First and foremost, this included re-instating the pre-2012 domestic workers' rights, which allowed workers to renew their visas and to ensure there was a route to settlement. The current visa regime creates unnecessary precarity which opens up MDWs to various on- and offline abuses from their employers, people in their social circles, and law enforcement. This has a direct impact on workers' privacy and security. For example, it would be relatively easy for a worker to confront their employer about surveillance if that worker had secure 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" [53]. This may reflect the politicised nature of VoDW as well as illustrate potential risks of universalising different migrant people's experiences across different countries, nationalities, and legal situations. There may be significant variations even within any group of people, and qualitative research often does not aim for generalisation.

The government and employers must take responsibility for protecting workers' privacy and safety. The government needs to work with grassroots organisations like VoDW and Migrants Organise 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.

Secondly, the UK law on indoor surveillance devices needs more clarity with regard to workers whose workplace is in someone else's household. There needs to be a clear prohibition of covert, non-consensual surveillance of domestic workers. Clear routes for restitution in cases of invasive recording or unnecessary data sharing are also needed. 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 to 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 (see §4.1.1). Similarly, police sharing data of victims of crime with immigration enforcement can leave

migrants fearful of reporting 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.

5.2 Implications and future research

5.2.1 Methodological recommendations

Build with existing community sources of safety and trust. Many of the most significant sources of safety in MDWs' lives are not necessarily technical but social and communal like membership in community support networks (see §4.3). In a situation where MDWs often could not 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 [4], refugees [105], sex workers [111], and queer people [48], demonstrating the importance of community support groups and collective security. Instead of suggesting new technical solutions in isolation from practitioners on the ground, digital security researchers can build on top of these existing sources of safety by partnering with community organisations to develop their information security capacity [109]. Participatory action research offers researchers a method to implement this.

Employ participatory action research as a security method. Methods like PTM offer a way to understand the power imbalances described above and centre marginalised communities' experiences. 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 threats 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, and security, and what methods and mechanisms they employ to defend against those perceived threats. Future research should seek to further distill 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. However, security researchers should take care to avoid research partnerships that are extractive or cause harm to the communities they intend to support [125].

Create pragmatic resources for participants. 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. The participatory action research method, 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 online because many domestic workers are turning to social media as their way to ease their isolation and vulnerability.*" This supports calls from past research for "community-appropriate educational resources" [53]. 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*" [55] onto those already burdened by precarity and abuse. This is why legal change and structural reform are also necessary for meaningful safety.

With regard to our own digital privacy and security guide, we believe it is crucial to translate the guide into other languages, such as Tagalog, which can increase the reach of this information and make it more beneficial for the communities whom it best serves. To continue to improve the guide, we would also encourage members of the privacy and security community to provide feedback. We also see the need for organising workshops with MDWs on the issues of privacy and security. In the past, Reconfigure ran feminist cybersecurity workshops [108], which could provide advice in a more personalised setting, as well as respond to topical changes (e.g., changes in the privacy policies of tech firms). Such workshops would also generate questions and key points for future guides. We have organised one follow-up workshop with VoDW to disseminate the guide and get feedback.

Advise employers. Alongside updated and translated guides for MDWs, we believe that a guide for employers could be beneficial in circumstances where employers may not be aware of how technology can violate their employees' rights or, indeed, what their employees' legal rights are at all.

Include users from a variety of backgrounds in user studies. Users have different privacy and security needs based on different life experiences. Aggregate descriptions of a population tend to obscure hidden populations such as MDWs, who may be more difficult to include in research. In missing communities like MDWs, security research will also miss the specific needs of and threats faced by these populations and, therefore, leave key vulnerabilities unaddressed.

5.2.2 Design implications

Balance the needs of device owners and other stakeholders. Technical interventions that help protect the safety and privacy of MDWs and marginalised communities include designing access control mechanisms and privacy settings that MDWs

can configure to protect their privacy [133]. Past research with survivors of IPV has shown the importance of robust multi-user security and privacy controls as well as designing surveillance devices to make it more obvious when they are on through visual or auditory clues. [71]. Crucially, such configurations should not only prioritise the home or device owner. Existing literature [132] only discusses use cases like "only allowing guests and domestic workers to access smart home devices while in the house".

However, the findings we reported on CCTV camera data ownership (see §4.1.3) show that domestic workers may need to use footage to document abuse. This would likely only be possible if workers could access this footage after leaving the physical premises of the house, perhaps because they left exploitative employment. 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. Access control policies and mechanisms should include the possibility of sharing data with 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.

Minimise opportunities for covert surveillance. In line with past findings [15, 63], we found that our MDW participants were very uneasy with the existence of secret recording devices (§4.1.3). Device manufacturers should not produce cameras and other surveillance devices meant to be hidden for the consumer market; 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. Prior work has found that signalling mechanisms and bystanders' ability to control data collection in some way had a significant effect on acceptability [30, 34, 47, 106, 107, 120].

Make privacy settings accessible. The experiences of MDWs highlight how critical social media settings and controls like restricting posts to only certain trusted members can be (see §4.3). For vulnerable groups like MDWs, this is not only a matter of privacy but can also impact their psychological, financial, and physical security. Past research with survivors of IPV has shown the importance of robust multi-user controls. Therefore, it is important that such controls are designed to be easily comprehensible and accessible to a variety of groups through, for example, translating them into multiple languages and avoiding jargon. Prior work has found that bystanders have misunderstandings of and misconceptions about device data practices, even if they are aware of the existence of devices in their environment [2, 81]. Even when bystanders understand the implications of different data practices, they do not have ways to express their privacy preferences [2, 15, 63, 81, 127].

Nudge employers towards ethical device use. Some employers may not be 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 that these devices should not be located in private or intimate places like bedrooms or bathrooms, informing them that doing so would be illegal as well as unethical. Similarly, they could remind users to inform other people in the house about recording devices and prompt them to ask for consent before recording others. This may increase transparency and ethical behaviour, which in turn improves workplace 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 like monitoring.

Stop developing harmful surveillance systems. 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 (see No Tech for Tyrants[11]). We argue security researchers must consider and seriously weigh the impacts that the development of surveillance technologies may have on the most marginalised people. As such, we call on researchers to avoid developing surveillance systems and collaborating with border enforcement entities.

6 Conclusion

Using the method of PTM with 32 MDWs in the UK, we define a threat model for MDWs, which includes intertwined and reinforcing threats: immigration surveillance, online scams and harassment, and employer monitoring. These threats leave MDWs vulnerable and isolated from broader society and critical services like healthcare. While community and social support networks such as VoDW provide a source of safety against these threats, digital privacy and security research needs to consider marginalised communities like MDWs. Threats to individual privacy and safety are exacerbated by offline societal issues like hostile immigration policies. We must collaborate with vulnerable populations when designing security frameworks and legal guidelines to ensure no one is left behind. Instead of becoming victims trapped in hidden surveillance, communities like MDWs can be active participants in creating a safer digital world.

Acknowledgements

This project would not exist without the contributions of community partners and workshop participants throughout the project. We also thank our reviewers and shepherd, as well as Natalie Sedacca, for helpful comments. This work was supported in part by a UK Research & Innovation grant (BB/T018593/1).

[11] https://notechfortyrants.org/

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 451–466, Santa Clara, CA, USA, 2019.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW):1–28, 2020.

[3] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. Up to a limit?: Privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(3):89:1–89:27, September 2018.

[4] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in large-scale urban protests: The case of Hong Kong. In *USENIX Security Symposium (USENIX Security)*, pages 3363–3380, August 2021.

[5] Noura Aleisa and Karen Renaud. Privacy of the Internet of Things: A systematic literature review. In *Hawaii International Conference on System Sciences (HICSS)*, 2017. Extended version available at https://arxiv.org/abs/1611.03340.

[6] Irwin Altman. *The environment and social behaviour: Privacy, personal space, territory, and crowding*. Brooks/Cole Publishing Company, 1975.

[7] Mark Andrejevic. Big data, big questions: The big data divide. *International Journal of Communication*, 8(0), 2014.

[8] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home Internet of Things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(2), June 2018.

[9] Till Ballendat, Nicolai Marquardt, and Saul Greenberg. Proxemic interaction: Designing for a proximity and orientation-aware environment. In *ACM International Conference on Interactive Tabletops and Surfaces (ITS)*, pages 121–130, 2010.

[10] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. Do privacy and security matter to everyone? Quantifying and clustering user-centric considerations about smart home device adoption. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 417–435, August 2020.

[11] Scott Beach, Richard Schulz, Julie Downs, Judith Matthews, Bruce Barron, and Katherine Seelman. Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey. *ACM Transactions on Accessible Computing*, 2(1):5:1–5:21, May 2009.

[12] Johanna Bergman and Isabelle Johansson. The user experience perspective of Internet of Things development. Master's thesis, Certec, Department of Design Sciences, LUND University, Lund, Sweden, 2017.

[13] Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rassmus-Gröhn. An exploratory study on how Internet of Things developing companies handle user experience requirements. In *Requirements Engineering: Foundation for Software Quality*, volume 10753 LNCS, pages 20–36, Germany, 2018.

[14] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, Boston, MA, USA, 2022. To appear.

[15] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, August 2020.

[16] Clara Berridge and Terrie Fox Wetle. Why older adults and their children disagree about in-home surveillance technology, sensors, and tracking. *The Gerontologist*, 60(5):926–934, 2020.

[17] Nellie Bowls. Thermostats, locks and lights: Digital tools of domestic abuse. *New York Times*, June 2018. Accessed: 23 July, 2018.

[18] danah boyd and Kate Crawford. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication, & Society*, 15(5):662–679, 2012.

[19] Virginia Braun, Victoria Clarke, Nikki Hayfield, Naomi P. Moller, and Irmgard Tischner. *Qualitative story completion: A method with exciting promise*. Springer, 2017.

[20] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place*, 50:112–118, 2018.

[21] George Chalhoub. The UX of things: Exploring UX principles to inform security and privacy design in the smart home. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, New York, NY, US, 2020.

[22] George Chalhoub and Ivan Flechais. "Alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In *International Conference on Human-Computer Interaction (HCII)*, 2020.

[23] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[24] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. Factoring user experience into the security and privacy design of smart home devices: A case study. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 1–9, New York, NY, USA, 2020.

[25] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *ACM Conference on Ubiquitous Computing (UbiComp)*, pages 61–70, 2012.

[26] Ian Clark. The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2, March 2016.

[27] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. How risky are real users' IFTTT applets? In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 505–529, August 2020.

[28] Kimberle Crenshaw. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stan. L. Rev.*, 43:1241–1299, 1991.

[29] Dana Cuomo and Natalie Dolci. Gender-based violence and technology-enabled coercive control in Seattle: Challenges and opportunities. *TECC Whitepaper Series*, 2019.

[30] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 2377–2386, New York, NY, USA, 2014.

[31] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J. Wisniewski. Exploring smart home device use by Airbnb hosts. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 1–8, New York, NY, US, 2020.

[32] Leen d'Haenens and Christine Ogan. Internet-using children and digital inequality: A comparison between majority and minority Europeans. *Communications – The European Journal of Communication Research*, 38(1):41–60, 2013.

[33] Ame Elliott and Sara Brody. Straight talk: New yorkers on mobile messaging and implications for privacy. Technical report, 2015. Accessed: 10 December, 2018.

[34] Barrett Ens, Tovi Grossman, Fraser Anderson, Justin Matejka, and George Fitzmaurice. Candid interaction: Revealing hidden mobile and wearable computing activities. In *ACM Symposium on User Interface Software & Technology (UIST)*, pages 467–476, Charlotte, NC, USA, 2015.

[35] Cori Faklaris, Francesco Cafaro, Asa Blevins, Matthew A O'Haver, and Neha Singhal. A snapshot of bystander attitudes about mobile live-streaming video in public settings. In *Informatics*, volume 7, page 10. Multidisciplinary Digital Publishing Institute, 2020.

[36] Jonathan Follett. *Designing for emerging technologies: UX for genomics, robotics, and the Internet of Things*. O'Reilly Media, Inc., 2014.

[37] Organization for Security and Cooperation in Europe (OSCE). Unprotected work, invisible exploitation: Trafficking for the purpose of domestic servitude: https://www.osce.org/secretariat/75804, 2011.

[38] The Joint Council for the Welfare of Immigrants (JCWI). The hostile environment explained: https://www.jcwi.org.uk/the-hostile-environment-explained, 2020.

[39] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "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), 11 2019.

[40] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise": How intimate partner abusers exploit technology. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–13, New York, NY, USA, 2018.

[41] Alisa Frik, Julia Bernd, Noura Alomar, and Serge Egelman. A qualitative model of older adults' contextual decision-making about information sharing. In *Workshop on the Economics of Information Security (WEIS)*, 2020.

[42] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, USA, 2019.

[43] Maria Gallotti. Migrant domestic workers across the world: Global and regional estimates. *International Labour Organization (ILO)*, 2015.

[44] Jon P. Gant, Nicole E. Turner-Lee, Ying Li, and Joseph S. Miller. National minority broadband adoption: Comparative trends in adoption, acceptance and use. Technical report, Joint Center for Political and Economic Studies, Washington, DC, USA, February 2010.

[45] Vaibhav Garg, L. Jean Camp, Lesa Lorenzen-Huber, Kalpana Shankar, and Kay Connelly. Privacy concerns in assisted living technologies. *Annals of Telecommunications*, 69(1):75–88, 2014.

[46] Bev Gatenby and Maria Humphries. Feminist participatory action research: Methodological and ethical issues. *Women's Studies International Forum*, 23, 1 2000.

[47] Jun Ge. Observers' privacy concerns about wearable cameras. Master's thesis, Pennsylvania State University, 2016. Masters thesis.

[48] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice. In *USENIX Security Symposium (USENIX Security)*, Boston, MA, USA, August 2022.

[49] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. Exploring consumers' attitudes of smart TV related privacy risks. In *International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*, Lecture Notes in Computer Science, pages 656–674. Springer, 2017.

[50] Maya Goodfellow. *Hostile environment: How immigrants became scapegoats*, volume 1. Verso Books, 2 edition, 2020.

[51] Stacey Gray. Always on: Privacy implications of microphone-enabled devices. Technical report, Future of Privacy Forum, April 2016.

[52] Rebecca Green and Michele Gilman. The surveillance gap: The harms of extreme privacy and data marginalization. *NYU Review of Law & Social Change*, 42, 2020.

[53] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–15, New York, NY, USA, 2018.

[54] Eszter Hargittai and Eden Litt. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy*, 11(3):38–45, May 2013.

[55] Bridget A. Harris and Delanie Woodlock. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59:530–550, April 2019.

[56] Claude PR. Heath, Peter A. Hall, and Lizzie Coles-Kemp. Holding on to dissensus: Participatory interactions in security design. *Strategic Design Research Journal*, 11, 2018.

[57] Chris Hoffman. What is an "evil maid" attack, and what does it teach us? *How-To Geek*, 2020.

[58] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 7057–7069, New York, NY, USA, 2017.

[59] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. Privacy behaviors of lifeloggers using wearable cameras. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 571–582, New York, NY, USA, 2014.

[60] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. End users' information-sharing behaviours and preferences within a multi-user smart home. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2020. Poster.

[61] Information Commissioner's Office (ICO). Domestic CCTV systems - guidance for people using CCTV: https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv, December 2021.

[62] International Labour Organization (ILO). Convention C189 - domestic workers convention, 2011 (no. 189), 2011.

[63] Mark Johnson, Maggy Lee, Michael McCahill, and Ma Rosalyn Mesina. Beyond the 'all seeing eye': Filipino migrant domestic workers' contestation of care and control in Hong Kong. *Ethnos*, 85, 2020.

[64] Kalayaan. 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/campaign-posts/dignity-not-destitution-the-impact-of-differential-rights-of-work-for-migrant-domestic-workers-in-the-national-referral-mechanism/, 2019.

[65] Marion Koelle, Wilko Heuten, and Susanne Boll. Are you hiding it?: Usage habits of lifelogging camera wearers. In *ACM International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*, pages 80:1–80:8, New York, NY, USA, 2017.

[66] Marion Koelle, Katrin Wolf, and Susanne Boll. Beyond LED status lights: Design requirements of privacy notices for body-worn cameras. In *ACM International Conference on Tangible, Embedded, and Embodied Interaction (TEI)*, pages 177–187, New York, NY, USA, 2018.

[67] Omead Kohanteb, Owen Tong, Heidi Yang, T Saensuksopa, and Saba Kazi. Decoding sensors: Creating guidelines for designing connected devices. Technical report, Carnegie Mellon University, Summer 2015. Accessed: 7 March, 2018.

[68] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 237–245, London, UK, 2002.

[69] Hosub Lee and Alfred Kobsa. Understanding user privacy in Internet of Things environments. In *IEEE World Forum on Internet of Things (WF-IoT)*, pages 407–412, December 2016.

[70] Linda Lee, Joong Hwa Lee, Serge Egelman, and David Wagner. Information disclosure concerns in the age of wearable computing. In *NDSS Workshop on Usable Security (USEC)*. Internet Society, 2016.

[71] Roxanne Leitão. Digital technologies and their role in intimate partner violence. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, New York, NY, USA, 2018.

[72] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *ACM Conference on Designing Interactive Systems (DIS)*, page 527–539, New York, NY, USA, 2019.

[73] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 'Internet of Things': How abuse is getting smarter. *Safe - The Domestic Abuse Quarterly*, 2019.

[74] Deborah Lupton. Self-tracking cultures: Towards a sociology of personal informatics. In *ACM Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design*, pages 77–86, New York, NY, USA, 2014.

[75] Mary Madden, Michele E. Gilman, Karen Levy, and Alice E. Marwick. Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, 95(1):53–125, 2017.

[76] Mary Madden and Lee Rainie. Americans' attitudes about privacy, security, and surveillance. Technical report, Pew Research Center, May 2015. Accessed: 9 February, 2018.

[77] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What *can't* data be used for?" Privacy expectations about smart TVs in the U.S. In *European Workshop on Usable Security (EuroUSEC), London, UK*, 2018.

[78] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2019(4):250–271, 2019.

[79] Lev Manovich. *Trending: The promises and the challenges of big social data*, pages 460–475. The University of Minnesota Press, Minneapolis, MN, USA, 2011.

[80] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(2):436 – 458, 2020.

[81] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "You just can't know about everything": Privacy perceptions of smart home visitors. In *International Conference on Mobile and Ubiquitous Multimedia (MUM)*, pages 83–95, 2020.

[82] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, New York, NY, US, 2020.

[83] Simon Moncrieff, Svetha Venkatesh, and Geoff West. Dynamic privacy in a smart house environment. In *IEEE International Conference on Multimedia and Expo (ICME)*, pages 2034–2037, 2007.

[84] Frances Montell. Focus group interviews: A new feminist method. *NWSA Journal*, 11, 1999.

[85] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 399–412, Santa Clara, CA, 2017.

[86] Ali Asghar Nazari Shirehjini and Azin Semsar. Human interaction with IoT-based smart environments. *Multimedia Tools and Applications*, 76(11):13343–13365, 2017.

[87] Carman Neustaedter and Saul Greenberg. The design of a context-aware home media space for balancing privacy and awareness. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 297–314. Springer, 2003.

[88] Home Office. Domestic workers who are victims of modern slavery - caseworker guidance, 2021.

[89] Jeungmin Oh and Uichin Lee. Exploring UX issues in quantified self technologies. In *International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, pages 53–59, 2015.

[90] Yong Jin Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, 2013.

[91] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In *New Security Paradigms Workshop (NSPW)*, pages 1–15, 2019.

[92] Scott R. Peppet. Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review*, 93:85–178, 2014.

[93] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 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, November 2018.

[94] James Pierce, Richmond Y. Wong, and Nick Merrill. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–19, New York, NY, USA, 2020.

[95] Alexander Ponticello. *Towards secure and usable authentication for voice-controlled smart home assistants*. PhD thesis, TU Wien, 2020.

[96] Halley Profita, Reem Albaghli, Leah Findlater, Paul Jaeger, and Shaun K. Kane. The AT effect: How disability affects the perceived social acceptability of head-mounted display use. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 4884–4895, New York, NY, USA, 2016.

[97] Amreen Qureshi, Marley Morris, and Lucy Mort. Access denied: The human impact of the hostile environment | IPPR, 2020.

[98] Lee Rainie and Janna Anderson. The future of privacy. Technical report, Pew Research Center, December 2014. Accessed: 17 July, 2018.

[99] Laura Robinson and Brian K. Gran. No kid is an island: Privacy scarcities and digital inequalities. *American Behavioral Scientist*, 2018.

[100] Ignacio Rodríguez-Rodríguez, José-Víctor Rodríguez, Aránzazu Elizondo-Moreno, Purificación Heras-González, and Michele Gentili. Towards a holistic ICT platform for protecting intimate partner violence survivors based on the IoT paradigm. *Symmetry*, 12(1):37, 2020.

[101] Claire Rowland. UX and service design for connected products: https://iotuk.org.uk/wp-content/uploads/2018/06/ux-and-service-design-iotuk.pdf, June 2018.

[102] Joanna Rutkowska. Evil maid goes after truecrypt!, 2009. The Invisible Things Lab's blog: https://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html.

[103] Natalie Sedacca. Migrant domestic workers and the right to a private and family life. *Netherlands Quarterly of Human Rights*, 37, 2019.

[104] Avril Sharp. Comment: Victims of slavery are trapped in destitution by right to work restrictions - free movement: https://www.freemovement.org.uk/national-referral-mechanism-right-to-work-restrictions.

[105] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the United States. In *IEEE Symposium on Security and Privacy (SP)*, pages 409–423, 2018.

[106] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. You are being watched: Bystanders' perspective on the use of camera devices in public spaces. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 3197–3203, New York, NY, USA, 2016.

[107] Manya Sleeper, Sebastian Schnorf, Brian Kemler, and Sunny Consolvo. Attitudes toward vehicle-based sensing and recording. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 1017–1028, New York, NY, USA, 2015.

[108] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, New York, NY, US, 2021.

[109] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates' digital security practices. In *USENIX Security Symposium (USENIX Security)*, Boston, MA, USA, August 2022. To appear.

[110] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. I'm all eyes and ears: Exploring effective locators for privacy awareness in IoT scenarios. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–13, New York, NY, USA, 2020.

[111] Angelika Strohmayer, Jenn Clamen, and Mary Laing. Technologies for social justice: Lessons from sex workers on the front lines. In *ACM Conference on Human Factors in Computing Systems (CHI)*, page 1–14, New York, NY, USA, 2019.

[112] Michael Onuoha Thomas, Beverly Amunga Onyimbo, and Rajasvaran Logeswaran. Usability evaluation criteria for Internet of Things. *International Journal of Information Technology and Computer Science (IJITCS)*, 8(12):10–18, 2016.

[113] Joseph Turow, Lauren Feldman, and Kimberly Meltzer. Open to exploitation: America's shoppers online and offline. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2005. Accessed: 3 June, 2015.

[114] Joseph Turow, Michael Hennessy, and Nora Draper. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2015. Accessed: 24 February, 2018.

[115] Joseph Turow, Michael Hennessy, Nora Draper, Ope Akanbi, and Diami Virgilio. Divided we feel: Partisan politics drive Americans' emotions regarding surveillance of low-income population. Technical report, Annenberg School for Communication at the University of Pennsylvania, 2018. Accessed: 24 December, 2018.

[116] UNICEF. Good governance of children's data | UNICEF Office of Global Insight & Policy: https://www.unicef.org/globalinsight/good-governance-childrens-data.

[117] John Vines, Stephen Lindsay, Gary W. Pritchard, Mabel Lie, David Greathead, Patrick Olivier, and Katie Brittain. Making family care work: Dependence, privacy and remote home monitoring telecare systems. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 607–616, 2013.

[118] Nina Wallerstein, Michael Muhammad, Shannon Sanchez-Youngman, Patricia Rodriguez Espinosa, Magdalena Avila, Elizabeth A. Baker, Steven Barnett, Lorenda Belone, Maxine Golub, Julie Lucero, Ihsan Mahdi, Emma Noyes, Tung Nguyen, Yvette Roubideaux, Robin Sigo, and Bonnie Duran. Power dynamics in community-based participatory research: A multiple–case study analysis of partnering contexts, histories, and practices. *Health Education and Behavior*, 46, 2019.

[119] Xin Wang. The content security mechanism of smart TV broadcasting operating system. *Open Access Library Journal*, 2(11), 2015.

[120] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the US. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2016(3):172 – 190, 2016.

[121] Frances Webber. On the creation of the UK's 'hostile environment'. *Race & Class*, 60(4):76–87, April 2019.

[122] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. "Privacy is the boring bit": User perceptions and behaviour in the Internet-of-Things. In *IEEE Annual Conference on Privacy, Security and Trust (PST)*, August 2017.

[123] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Smart homes and their users: A systematic analysis and key challenges. *Personal and Ubiquitous Computing*, 19(2):463–476, February 2015.

[124] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Benefits and risks of smart home technologies. *Energy Policy*, 103:72–83, April 2017.

[125] Todd Wolfson, Ursula Elin Huws, James M. Farrar, and Yaseen Aslam. 'Alongside but not in front': Reflections on engagement, disengagement and ethics in action research with workers. *Work Organisation, Labour & Globalisation*, 2022.

[126] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–12, New York, NY, USA, May 2019.

[127] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, November 2019.

[128] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Free to fly in public spaces: Drone controllers' privacy perceptions and practices. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 6789–6793, New York, NY, USA, 2017.

[129] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 6777–6788, New York, NY, USA, 2017.

[130] Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. Security analysis of Internet-of-Things: A case study of August smart lock. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017.

[131] Colin Yeo. The hostile environment: What is it and who does it affect? | New Europeans: https://neweuropeans.net/article/1927/hostile-environment-what-it-and-who-does-it-affect, 2017.

[132] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 65–80, Santa Clara, CA, 2017.

[133] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *USENIX Security Symposium (USENIX Security)*, pages 159–176, Santa Clara, CA, August 2019.

[134] Kai Zhao and Lina Ge. A survey on the Internet of Things security. In *International Conference on Computational Intelligence and Security (CIS)*, pages 663–667, 2013.

[135] Nicole Zillien and Eszter Hargittai. Digital distinction: Status-specific types of Internet usage. *Social Science Quarterly*, 90(2):274–291, 2009.

Appendix A: Workshop questions

The topics discussed in the workshops were as follows:

ASSETS:

1. What kinds of social media or communication technology do you use?
2. How do you feel about using social media and communication technology?
3. What parts of your data or information do you most want to protect?
4. What does being safe mean to you?

THREATS:

1. What are the main threats to your safety, privacy, and security (e.g., threats faced online or in your workplace)?
2. Have you ever worked in a house where there was a camera or some type of a monitoring device? If yes, how did you find out about it? How did you feel about it?
3. Are you worried about being watched online? If so, by who and why?

MITIGATIONS:

1. What advice would you give other MDWs to stay safe online?
2. What parts of your safety do you most want to improve?
3. Do you have any questions you want to ask us?
4. What kind of support do you need to be safe?

Appendix B: Digital privacy and security guide

Based on the findings of our five workshops with MDWs in the UK, we developed a digital privacy and security guide. The guide serves as an educational/support platform for MDWs in the UK and other countries, to protect their on- and offline privacy and keep themselves safe. The guide is divided into six main sections. We first explain the guide and its purpose; provide general digital privacy and security advice; describe three main types of privacy threats identified by our MDW participants who took part in our workshops (one section is dedicated to each threat type): government surveillance, online scams and harassment, and employer monitoring; and conclude by arguing that our computer security and privacy community must take into account intersecting forms of marginalisation (due in part to different levels of social and economic power) as well as the broader social structures that foster insecurity. The guide also includes links to further resources that domestic workers can refer to when in need of protection.

About the guide. The first section of the guide explains its purpose: providing general information and advice on how MDWs can protect their privacy and safety. The guide is not a substitute for legal advice. The section also describes the academic institutions and grassroots organisations involved in developing this guide.

General digital privacy and security guide. The second section of the guide provides general advice on how to protect domestic workers' digital privacy and security. The advice includes thinking about and checking the links (and files) before clicking on (downloading) them, configuring the privacy settings of their online social accounts, and securing their online accounts and devices using a set of mechanisms and tools. This section includes resources and links explaining the steps that workers could find useful to achieve the above.

Immigration and government surveillance. The third section describes the first main threat identified by our MDW participants: government surveillance. Many participants reported a fear of government institutions, specifically the Home Office and the police, due to the power these structures had over their immigration status and that of other workers. This section provides information about workers' rights with regard to accessing healthcare services like the NHS and seeking protection from excessive policing. It explains practical steps that domestic workers can take to protect their privacy and human rights (e.g., joining grassroots organisations and unions, contacting legal aid organisations and law centres), what to do if immigration officers or the police stopped them to enquire about their immigration status, and what resources they can use to access healthcare services, get legal advice, and navigate the Home Office hostile environment.

Online scams and harassment. The fourth section explains the second threat type described by our participants: scams, identity theft, and harassment. MDWs can be specifically targeted by scams due to their immigration status; e.g., scammers might offer fake job opportunities or threaten to report workers to the Home Office. This section provides useful resources as well as customised advice on how domestic workers can recognise scams, get their money after they have been scammed, and how to protect themselves from identity theft and online harassment.

Employer monitoring. Constant CCTV surveillance of employees/workers or social media stalking can be a huge threat to domestic workers' privacy and security. The fifth section describes workers' legal rights with regard to what employers can and cannot do. It also provides practical advice on how to protect from employer monitoring, such as avoiding adding employers as friends on social media, identifying where cameras and other monitoring devices are located in their workplace, and having a conversation with their employers about the purpose and use of cameras.

Broader changes. The final section of the guide argues that domestic workers should not be blamed for the digital privacy and security threats we described in this guide. Our computer security and privacy community, the government, and employers have their own responsibilities for protecting the safety and privacy of workers. The computer security and privacy community must consider intersecting forms of marginalisation as well as the broader social structures that foster insecurity. The government needs to work with grassroots organisations including VoDW to improve the conditions of workers in the UK, create a safe environment, and protect their human rights. Employers need to understand and respect domestic workers' right to privacy and safety, and refrain from excessive monitoring. The section concludes with useful contacts that domestic workers can use when in need of protection.