Working at the Frontline: Privacy, Security, and Everyday Labour of Immigration Caseworkers

Arshia Dutta*, Atmadeep Ghoshal†, Martim Brandão†, Ruba Abu-Salma†
*Royal Holloway, University of London
Email: arshia.dutta.2023@live.rhul.ac.uk
†King's College London
Emails: {atmadeep.ghoshal, martim.brandao, ruba.abu-salma}@kcl.ac.uk

***Abstract*—Immigration caseworkers supporting migrants, refugees, and asylum seekers in the UK handle some of the most sensitive personal information in frontline support work, yet the privacy and security dimensions of their labour remain largely unexamined. Drawing on a mixed-methods study comprising semi-structured interviews, field observations, and a workshop with caseworkers at migrant support organisations in and around the UK, this study examines how caseworkers negotiate privacy and security through everyday practices of judgement, care, and risk management. We find that caseworkers enact security as a form of humanitarian care for people whose circumstances depend on institutional processes that are unreliable and consequential. This orientation shapes their security practices in ways that existing frameworks of situated and usable security cannot fully account for. We further find that structural security gaps arising from resource scarcity, concentrated technical knowledge, and the absence of formal policies leave organisations and clients exposed to risks that individual commitment cannot address. This study contributes to HCI and usable security research by foregrounding the overlooked labour involved in protecting vulnerable clients, sensitive information, and support organisations, and by showing how security practices in these settings are shaped by the commitments of those involved and the political climate in which they work.**

1. Introduction

Immigration casework in the United Kingdom involves the routine handling of some of the most sensitive personal information encountered in frontline support contexts [1]. Caseworkers at migrant support organisations help individuals navigate asylum claims, refugee resettlement, and a range of immigration processes that are administratively complex and nearly impossible to manage without specialist assistance. In doing so, they make representations to the Home Office, the government department responsible for immigration, policing, and national security, on behalf of clients. They assemble documentation for legal proceedings, correspond with housing providers, solicitors, and partner charities, and help clients manage their immigration status through processes requiring detailed personal, biographical, and legal information [2]. These tasks make caseworkers more than administrative intermediaries. They become directly responsible for how vulnerable clients are made visible, credible, and actionable within institutions that determine their access to status, housing, welfare, legal protection, and physical safety. The sensitivity of this information is compounded by the precarious conditions under which caseworkers operate. Migrant support organisations typically manage complex caseloads with limited funding, small or volunteer-dependent teams, and few, if any, formal security policies [3]. Serving marginalised populations, these organisations often develop security practices based on perceived rather than measured risks, leaving persistent gaps between formal protections and everyday operational requirements [4]. Organisational security and client safety are therefore mutually entangled rather than separable in these settings [5], an entanglement that is continually reflected in everyday practice.

Furthermore, the clients whom caseworkers support face distinct forms of vulnerability that conventional privacy and security frameworks struggle to capture. Previous work across diverse geopolitical contexts has highlighted these systemic gaps. For instance, research with refugees settling in Sweden demonstrates that the immediate need to access digitally mediated resettlement services is routinely prioritised over privacy and security concerns, exposing individuals to risks they can neither assess nor resist [6]. A decade-long review of migration research in HCI similarly documents the persistent challenges that forced migrants face when accessing host-country digital infrastructures [7]. Beyond forced migration, research on migrant domestic workers in Chinese smart homes has shown that employer-controlled surveillance technologies reinforce a sense of constant monitoring, further amplifying worker vulnerability [8]. Related work confirms that these dynamics extend to smart environments in which workers have little or no control over the technologies monitoring them [9]. In the UK, participatory threat modelling with migrant domestic workers has further illustrated how structural power asymmetries between workers and employers shape both exposure to harm and the practical feasibility of protective action [10]. Research with marginalised populations in Lebanon has similarly shown that, where governance fails and institu-

tional infrastructure is weak, protection cannot be achieved systemically. Instead, people must piece together safety from whatever informal, partial, and heterogeneous resources are available [11], [12]. Immigration casework sits within this fragmented and asymmetric landscape, but with a critical difference: caseworkers bear the additional responsibility of actively handling the documents, accounts, communications, and disclosures through which client privacy and security risks are reduced, intensified, or redirected. This protective work closely resembles practices documented in other frontline settings where formal infrastructure is limited. Advocates supporting survivors of domestic violence develop intertwined emotional, organisational, and technical security practices that extend well beyond formal training [13]. These practices form networks of care through which advocates build relationships across services and stakeholders to create more supportive environments for survivors [13]. Similar dynamics have been documented among victim service providers supporting survivors of human trafficking [14], computer security support staff encountering technology-facilitated abuse [15], and in domestic labour settings where employer-controlled smart home technologies create conditions of pervasive monitoring [9], reshaping workers' sense of safety and autonomy in their working environments [8]. Across these settings, security is enacted through care and constraint, shaped by the need to protect others while working with limited authority, incomplete infrastructure, and risks that exceed standard technical models.

Yet immigration caseworkers remain largely absent from this literature, particularly regarding how they manage the privacy and security dimensions of client-facing information work and how they and their organisations navigate the organisational and personal risks associated with frontline immigration support. This study addresses this gap by examining how privacy, security, and personal safety are negotiated in the everyday work of immigration caseworkers in England. Drawing on semi-structured interviews, field observations at migrant support organisations, and a co-design workshop on AI, privacy, and security in immigration casework, we investigate two research questions. **RQ1** asks: How do caseworkers encounter and manage privacy and security risks in client-facing work? **RQ2** asks: What privacy and security risks do caseworkers and their organisations face in their own right?

Our findings show that caseworkers enact security as a form of humanitarian care. They protect documents, manage consent, limit unnecessary disclosure, respond to institutional errors, assess suspicious communications, and reduce their own public visibility because they recognise that a client's ability to be believed depends on how their data is handled. This orientation is rooted in a commitment to lawful, impartial processes and shaped by the political climate surrounding their work, influencing security practices in ways that existing frameworks of situated and usable security cannot fully capture. We further find that this protective work is sustained by fragile organisational arrangements. Structural security gaps arising from resource scarcity, concentrated technical knowledge, informal routines, limited incident reporting, and the absence of formal policies leave organisations and clients exposed to risks that individual commitment alone cannot address. Our study contributes to HCI and usable security research by foregrounding the overlooked labour involved in protecting vulnerable clients, sensitive information, and support organisations. It shows how security practices in these settings are shaped by the humanitarian care and commitment to lawful processes that underpin caseworkers' work. Strengthening security in migrant support settings therefore requires more than technical capacity-building. It demands shared organisational infrastructure capable of sustaining protective practices through staff transitions, resource pressures, and the structurally precarious conditions of frontline immigration work.

2. Related Work

2.1. Privacy and Security for Migrants and Marginalised Populations

Prior work has shown that migrants, refugees, and asylum seekers encounter digital privacy and security risks that are poorly captured by standard threat models. Refugees resettling in the United States relied heavily on technology while facing cultural, linguistic, and institutional barriers that made common security practices difficult to apply. Security was often subordinated to more immediate needs, such as finding employment [16]. Undocumented immigrants remained highly attentive to offline threats while expressing resignation towards forms of digital surveillance that they could neither assess nor meaningfully resist [17]. Immigrants moving to the United States similarly negotiated difficult trade-offs between privacy, security, and integration, often accepting exposure in order to access essential services [18]. Participatory threat modelling with migrant domestic workers in the United Kingdom further demonstrated how structural power asymmetries shaped both exposure to harm and the feasibility of protective action, identifying government surveillance, employer monitoring, and online harassment as the most salient threats [10].

Research on privacy and security among marginalised populations more broadly has highlighted the structural conditions that produce these risks. Sannon et al. (2022) characterise the field as fragmented and population-specific, arguing for approaches that address the conditions producing vulnerability rather than treating it as an inherent property of particular groups [19]. Warford et al. (2022) identify contextual risk factors, including marginalisation and access to sensitive resources, that intensify digital safety risks across diverse populations and can inform the design of interventions [20]. Research with survivors of intimate partner violence has been particularly important in demonstrating that security support often operates through care relationships rather than technical tools alone. Studies have documented survivor practices [21], clinical consultation models [22], the broader landscape of technology abuse [23], and the sociotechnical infrastructure needed to sustain

security support over time [24]. Across these studies, privacy and security risks are shown to be shaped by legal precarity, institutional dependence, social relationships, and unequal access to protection. However, the experiences of frontline workers who mediate between migrants and the institutions that govern their lives remain under-examined. These workers do not simply transmit information on behalf of clients. They interpret, protect, and negotiate highly sensitive material under conditions of legal uncertainty and organisational constraint, while also facing privacy and security risks of their own. Our study addresses this gap by examining caseworkers as subjects of privacy and security in their own right, rather than merely as intermediaries through whom migrants' experiences can be understood.

2.2. Casework, Frontline Labour, and Information Practice

CSCW and HCI research has developed a rich understanding of the data and information labour performed by frontline workers in mission-driven and resource-constrained organisations. A fundamental insight in this tradition is that some of the most consequential work in collaborative settings remains invisible: it is carried out to make formal systems function but rarely appears in official records, workflows, or job descriptions [25]. In data-driven long-term care settings, Sun et al. (2023) show that frontline care workers perform extensive maintenance, articulation, and repair work to keep data technologies usable in practice, even though this work is largely absent from institutional accounts [26]. Bopp et al. (2017) similarly find that data-driven reporting requirements constrain rather than empower non-profit organisations, as funder demands redirect attention away from the priorities of the communities they serve [27]. In related work, they find that non-profits remain under-represented even in HCI studies that claim to address their needs, calling for more participatory and organisationally attentive forms of engagement [27].

Studies of everyday information management in non-profits document how improvised data systems emerge alongside, and sometimes in place of, formal infrastructures, serving not merely as workarounds but as primary means of meeting operational needs. For instance, Voida et al. (2011) show that non-profit workers routinely maintain home-grown databases outside official systems, reflecting a persistent gap between organisational infrastructure and everyday needs [28]. Dombrowski et al. (2014) find that outreach workers absorb the complexity of institutional systems on behalf of clients who cannot navigate them alone, taking on technical, relational, and advocacy roles that formal systems neither recognise nor resource [29]. Erete et al. (2016) show that non-profits working with open data develop narrative practices to translate complex information into forms that funders and stakeholders can use, requiring substantial interpretive work that is rarely recognised as part of the organisation's core activities [30]. Voida et al. (2012) find that volunteer coordinators occupy a difficult intermediary position between organisations and the public, managing information flows across multiple parties with limited formal guidance and absorbing relational labour that formal systems do not account for [31]. In workplace contexts more broadly, Chowdhary et al. (2023) show that consent is weakened by structural power asymmetries, with tacit compliance frequently displacing meaningful agreement in ways that erode workers' capacity to make genuinely informed decisions [32]. Saxena et al. (2021) extend this concern by showing that, in public-sector welfare settings, risk and accountability are distributed unevenly, with frontline workers absorbing responsibility for decisions shaped by systems they did not design and cannot fully interrogate [33].

Despite this rich body of work, the privacy and security dimensions of invisible frontline labour remain under-examined, particularly in settings where the information being handled concerns people whose legal status, safety, and access to services make exposure especially consequential. We build on this work by approaching immigration casework as security-sensitive information labour, attending both to what caseworkers protect and to the conditions that do or do not protect them.

2.3. Organisational Security, Digital Threats, and Everyday Security Practice

Human-centred security research has shown that protection in non-expert and resource-constrained settings often depends on informal knowledge, social relationships, and situated judgement rather than formal controls alone. In domestic settings, incident stories shared by family and friends shaped how people understood threats and decided what action to take [34]. Security knowledge also varied by source, with peer accounts, expert webpages, and news articles framing everyday risks in different ways [35]. This complicates the assumption that more information automatically leads to safer behaviour. Security beliefs do not always translate into protective action [36], and people often rely on trusted social networks when institutional guidance is absent [37]. Users' mental models of threats may diverge from technical accounts while remaining coherent within everyday practice [38]. These capacities are also unevenly distributed, with socioeconomic status influencing sources of advice, protective knowledge, and security practices [39]. At the same time, non-expert users should not be understood solely in terms of their limitations, as they also bring contextual and relational knowledge to tasks such as phishing detection [40].

At the organisational level, security practices are shaped by professional routines, institutional pressures, and the demands of daily work. Research with journalists showed that security tools were resisted when they disrupted source communication and editorial workflows, indicating that interventions must fit the cultures and conditions in which they are used [41]. Research on phishing awareness in a German public-sector organisation further showed that training effects weaken without reinforcement, limiting the value of one-off interventions [42]. Research with a large humanitarian organisation similarly showed that NGOs face

distinctive risks because they must remain accessible while protecting sensitive beneficiary data [43]. This literature establishes that security is socially organised, unevenly resourced, and deeply shaped by context. However, it has not fully examined organisations that support politically exposed and legally vulnerable populations amid chronic resource scarcity, hostile public attention, and limited technical expertise. Our study addresses this gap by examining how migrant support organisations manage security in practice and how caseworkers navigate responsibilities that connect their own safety, organisational capacity, and the protection of clients whose information they hold.

3. Methodology

Our study was conducted across three organisations that had received Independent Assurance Accreditation and were classified as Level 1 or Level 2 organisations, a legal classification that participants themselves emphasised when describing the standing and accountability of the charities involved. To address RQ1 and RQ2, we adopted a sequential, multi-stage design combining field observations, unstructured interviews, a workshop, and semi-structured interviews. Each stage built on the findings of the preceding stage. Observations and unstructured conversations provided grounded familiarity with the physical arrangements and everyday pressures of casework, informing the materials and focus of the workshop. The workshop brought caseworkers from different organisations together to discuss shared concerns, generating reflections that individual conversations alone could not have elicited. These reflections, in turn, shaped the focus of the subsequent semi-structured interviews. This sequential design allowed us to move from observation to collective dialogue to individual reflection, progressively deepening our understanding of how privacy and security are negotiated in everyday casework.

3.1. Participant Recruitment and Data Collection

3.1.1. Research Access and Organisational Engagement. We contacted seven organisations supporting refugees and migrants across different regions of England. One organisation had an existing relationship with the research team, as one researcher had previously volunteered there. This organisation served as an initial point of access, connecting us to a further six organisations through snowball referrals. We initially contacted these six organisations through cold emails introducing the research focus and our intention to spend time understanding the everyday realities of casework before making any formal data requests. Through our experience working with migrant support organizations, we had learned that arriving solely to collect data could feel extractive. Therefore, we made it clear in our outreach that observation and organizational familiarity were as central to the study as data collection. Two of the six organisations responded positively and, together with the organisation we already knew, ultimately participated in the study. The cold emails outlined our interest in the privacy and security dimensions of immigration casework while also making clear that we wanted to understand the broader pressures and service contexts within which caseworkers operated. This positioning was deliberate. Immigration casework involves highly sensitive material and unequal power relations, and we recognised that approaching organisations as researchers asking about security vulnerabilities without first establishing trust could feel threatening. Building organisational familiarity before making formal requests was therefore as much a methodological decision as an ethical one.

3.1.2. Exploratory Conversations with Caseworkers. During this early period of engagement, we conducted unstructured interviews [44] with seven caseworkers as part of our efforts to understand the field. These conversations were not designed to generate data in the conventional sense, and our notes from them were not coded as part of the analysed corpus. Instead, they helped us understand which aspects of casework raised the most significant privacy and security concerns, how caseworkers described these concerns in their own terms, and which institutional actors and technological systems featured most prominently in their everyday work. The insights gathered during these conversations directly informed the design of the semi-structured interview guide used in the later stage of the study. This exploratory phase also allowed caseworkers to become familiar with us and the study's focus. This was important because the topics we were asking about, including organisational vulnerabilities, digital practices, and client confidentiality, required a degree of trust that could not be assumed simply because organisational access had been granted.

3.1.3. Field Observations. Field observations ran alongside these early conversations, with the objective of understanding the material realities of casework. Two members of the research team, including the researcher who had previously volunteered, spent time in casework spaces at three organisations, conducting three visits to each organisation over six months, from November to April. During these visits, we attended to the physical and material arrangements through which support was organised. We observed the layout of reception areas, waiting spaces, advice rooms, and training areas. We noted the presence and placement of CCTV cameras, electronic door locks, and other access control mechanisms. We also paid attention to seating arrangements, how caseworkers positioned themselves relative to clients and lawyers, and how people moved through the buildings over the course of a working day. These observations were analytically significant in their own right. They showed that privacy and security in casework were not enacted solely through digital systems or formal policies, but were also embedded in spatial arrangements, material infrastructures, and the daily rhythms of busy support organisations. They also gave us a more grounded understanding of the pressures caseworkers worked under and the security compromises organisations had to make in practice because of funding or infrastructural deficits, which we could not have understood from interviews alone.

3.1.4. Workshop Design and Facilitation. Data from our observations and unstructured interviews directly informed the design of a workshop that we subsequently conducted with caseworkers. Through the earlier phases of the study, we had developed a grounded understanding of individual caseworkers' experiences, but we could not yet understand how caseworkers across different organisations collectively made sense of shared concerns. The workshop was therefore designed to bring them together to discuss issues that had emerged during the earlier phases and to generate reflections that individual conversations alone could not produce. In particular, caseworkers had raised AI tools unprompted during the unstructured conversations, expressing concerns about their safety and privacy implications and a strong desire to understand them better. We felt that exploring these questions in a collective setting would elicit deeper and more critical engagement, so the workshop's focus on AI was grounded in participants' own concerns.

Drawing on what we had learned about caseworkers' everyday concerns through our observations and initial conversations, alongside prior work on AI risk and safety in high-stakes contexts such as immigration, we developed workshop materials focused on three areas that had emerged as particularly significant: the use of AI tools in casework and by state institutions; the privacy risks arising from fragmented services and institutional communication; and the security pressures caseworkers faced in their own right. We piloted these materials with four participants, and no substantial changes to their content or themes were requested during the pilots. The workshop brought twenty-one caseworkers from the three participating charities together for a single, full-day session in which they responded to scenarios and demonstrations drawn from their working contexts. The workshop comprised three sessions, each attended by all participants.

The first session drew on our field observations to discuss everyday casework challenges, including infrastructural constraints, funding pressures, and security practices we had observed that could inadvertently compromise client confidentiality. The second focused on AI tools in casework, covering both productive uses that caseworkers had developed and the associated risks. It also introduced open-source language models as a lower-cost alternative that participants had asked about, alongside an account of the privacy and security risks they pose. The third session addressed the broader implications of AI-based decision-making in immigration governance, focusing on how automated systems can produce decisions that are difficult for caseworkers to understand or challenge, and the practical burden this places on caseworkers when supporting clients through appeals. By this stage in the fieldwork, sustained engagement with participants during the earlier phases had established sufficient trust for the workshop to be audio-recorded and transcribed in full.

3.1.5. Semi-Structured Interviews. Following the workshop, we conducted semi-structured interviews with all twenty-one caseworkers who had participated in the workshop, drawing on prior HCI research with at-risk communities [45] to explore the issues that had emerged in greater depth. Our interview questions covered everyday information handling, data-sharing practices, communication tools, workplace privacy, system access, organisational rules, informal workarounds, perceived vulnerabilities, and situations in which caseworkers felt responsible for protecting client or organisational information. Broader details about immigration processes emerged in participants' accounts and were treated as context for understanding the security and privacy demands placed on caseworkers, rather than as findings in their own right.

3.1.6. Data Documentation and Ethical Handling. Two members of the research team took contemporaneous notes independently during the unstructured interviews and field observations, subsequently cross-checking their notes. The workshop was audio-recorded and transcribed in full, as participants had by that stage developed sufficient familiarity with the research team to consent to recording in a collective setting. For the semi-structured interviews, eighteen participants consented to audio recording, and verbatim transcripts were produced. Three participants preferred not to be recorded; for these interviews, we relied on detailed contemporaneous notes documenting key practices, examples, and reflections, recording direct quotations only where the wording had been captured with sufficient confidence. We understood this preference as reflecting the more sensitive and specific nature of the issues explored in individual interviews compared with the collective workshop discussion. All participants were subsequently given the opportunity to review the full materials attributed to them, including transcripts and notes, and to add, remove, or amend anything before the data was used for analysis.

3.1.7. Trust, Volunteering, and Researcher Positioning. Trust across all phases of the study was treated as something that had to be built and maintained rather than assumed. The research team had an existing relationship with one of the three participating organisations, where one researcher had previously volunteered. This prior connection facilitated initial access and helped establish credibility with the wider network of organisations that subsequently joined the study. We made clear that participation was voluntary, that the study was not an evaluation of individual performance, and that caseworkers could choose what they felt comfortable discussing. Verbal consent was obtained from all participants at the start of each phase of the study, and participants were reminded that they could withdraw from the study or request the removal of any part of their contribution at any point. All interviews took place during weekday working hours, at times and in spaces that suited participants. Over the course of the fieldwork, this sustained and careful engagement allowed caseworkers to speak about issues they described as sensitive, including the limits of their own security knowledge, the vulnerabilities of the systems they used, and the pressures they experienced while working in a politically hostile environment.

3.2. Data Analysis

We employed inductive thematic analysis following Braun and Clarke's six-phase framework [46]. Two researchers familiarised themselves with the complete corpus, comprising semi-structured interview notes and transcripts, observational field notes, and workshop transcripts, through repeated close reading and discussion. This process generated initial analytic observations about recurring concerns, including consent, data sharing, client vulnerability, AI use, institutional opacity, and staff safety. Both researchers then independently coded all materials, producing semantic codes such as *"clients sign consent forms," "documents stored in Charity Log,"* and *"caseworkers do not share phone numbers,"* alongside latent interpretive codes such as *"consent as fragile," "caseworkers as privacy filters,"* and *"visibility as organisational risk."* The researchers met regularly to compare codes, resolve discrepancies through discussion, and iteratively refine the codebook. Code saturation was reached after six rounds of discussion and refinement, at which point no new codes emerged from the data. Both researchers then applied the finalised codebook to all materials, resolving any remaining disagreements through consensus. Related codes were subsequently grouped into candidate themes to address our research questions, reviewed against the full dataset, and refined for coherence, distinctiveness, and analytic contribution. The final themes were named and defined with explicit scope, and detailed records of all analytic decisions were maintained throughout.

This collaborative approach supported rigorous and systematic analysis while remaining attentive to the social and organisational context of immigration casework. We acknowledge that participant sample size in qualitative research is debated [47] and that data saturation is inherently subjective [47]. We assessed saturation by iteratively refining our themes until the meanings necessary to address our research questions were fully captured. Our sample of 21 participants aligns with qualitative guidelines that prioritise depth over generalisability [48]. Because qualitative samples do not support claims about prevalence beyond the sample itself [49], we describe how widely a view or practice was held using terms such as some, many, and most, and report numbers only for the study design and sample in the methodology. We do not report participant-level demographics to protect participants in small organisations where individuals could be identified.

4. Findings

We present our findings in two connected parts. The first addresses RQ1 and documents how caseworkers encountered and managed privacy and security risks in client-facing work, covering the everyday structure of casework, the practical protection of client information, the fragility of consent processes, the downstream circulation of Home Office correspondence, and clients' use of AI tools. The second addresses RQ2 and documents the organisational and personal risks faced by caseworkers themselves, covering organisational invisibility as a security strategy, physical and digital security measures, organisational capacity constraints, and caseworkers' own use of AI. Finally, we describe the commitments and political climate shaping this work and summarise the protective strategies reported across both parts.

4.1. Privacy & Security in Client-Facing Casework

4.1.1. The Everyday Structure of Immigration Casework. During the workshop, participants described the everyday workflows of caseworkers supporting immigrants, refugees, and asylum seekers. Although practices varied across organisations, participants largely attributed these differences to financial hardship and infrastructure constraints rather than fundamentally different approaches to casework. Participants from a small charity in the north of England explained that they could not afford to offer walk-in services and therefore relied on scheduled appointments, noting that *"...it was only easier to see clients on scheduled dates since that would minimise their chances of being turned away should a caseworker be absent."* In contrast, participants from a well-funded urban charity described a more flexible model that combined walk-in appointments with proactive outreach to asylum seekers housed in government hotels. Across organisations, clients were typically introduced through informal referrals or partner charities. As one participant with three decades of experience explained, *"...there are only two ways we get introduced to our clients... either they get to know us from friends and family... the other way is that usually we have partner charities who have volunteers stationed at immigrant hotels... and they send them to us."*

The first stage of casework involved *decoding* clients' documentation. Asylum seekers often brought **bail judgements**[1] and **S95**[2] letters confirming temporary support entitlements, while refugees presented grant of leave letters and **UKVI**[3] correspondence confirming their legal status and rights. Once caseworkers had established a *"coherent idea about where their clients were coming from"*, they supported clients with a wide range of needs, including preparing Home Office applications, providing interview preparation, arranging food, medicine, and clothing, writing housing support letters, registering clients with GP surgeries, and assisting with travel documents and work licences. Reflecting on this work, one participant noted, *"...sometimes these people are coming from war-torn places...with kids....and we work hard to give them all that they need."*

1. Bail judgements in the immigration context are documents issued by the UK Home Office confirming that an asylum seeker has been granted temporary admission to the UK while their claim is being processed.

2. Section 95 of the Immigration and Asylum Act 1999 provides for the Home Office to support asylum seekers who would otherwise be destitute, covering accommodation and a small weekly financial allowance.

3. UK Visas and Immigration is the Home Office department responsible for making decisions about who has the right to visit or stay in the UK. Refugees and asylum seekers are issued a UKVI online account that serves as digital confirmation of their immigration status.

The privacy and security concerns identified through the workshop and interviews were embedded in these routine activities. Client meetings, referral pathways, Home Office correspondence, UKVI account details, housing documentation, medical registrations, and employment records all presented points at which caseworkers had to decide what information to collect, how to interpret it, where to store it, and when it could be safely shared. Privacy and security were therefore not separate concerns but integral to the everyday practices through which clients became visible to charities, partner organisations, and state institutions.

4.1.2. Protecting Client Information in Practice. Data related to clients, including the documents they brought to casework meetings, was identified by most participants as the most important site through which privacy and security concerns emerged in immigration casework. Yet before these documents became what caseworkers described as a 'point of absolute vulnerability', the initial interaction between caseworker and client was already a significant site of privacy and security concern. As one of our participants explained, *".....before we go through the documents, we hear from their stories and their sufferings and all the other details through which we make initial assessment of them in our minds...and that is a spot which we do not want anyone to take leverage of..."* Our workshops, initial observations, and subsequent interviews indicated that when clients visited a charity to meet a caseworker, either by appointment or as walk-ins, their interactions would usually take place in a secure space with minimal access for other staff members, even if they were caseworkers themselves. Often, when space was limited, particularly in charities facing funding constraints, these interactions would either be staggered to ensure that caseworkers spoke to one client at a time while others waited in a separate room, or take place with long wooden frames serving as temporary partitions between two caseworkers speaking to their respective clients. As these initial interactions often involved clients describing their journeys, caseworkers relied on trained interpreters to translate what their clients said. Some caseworkers pointed out that, during this process, they preferred not to have friends or family members perform the translation in order to preserve the originality and authenticity of their clients' experiences.

While caseworkers took notes whenever they spoke to their clients, we were told that these notes were almost immediately digitised after the interaction concluded and stored in the charity's designated computer file system, which was usually password-protected. Charities with greater financial resources used a tool called ***Charitylog***[4], which served the same purpose but offered a database- and CRM-oriented setup that allowed caseworkers to *"manage files more efficiently, track appointments across a specific year or month and protect client data with GDPR compliant software from the very beginning..."* During the research, caseworkers reported that Charitylog did not offer any AI-enabled features in their subscribed plans. Access to Charitylog was also password-protected for each individual user account. Caseworkers made copies of their clients' letters and other correspondence using their own in-house scanners. All the charities we engaged with as part of our research could afford printer-enabled scanners for their work. As we observed during our field visits, these scanners were placed close to the caseworkers' workspaces to prevent any form of information leakage. As one caseworker explained, *".....our desktops, scanners and telephones are all placed in close proximity to us so that we do not have to walk over to someone else's table to get things done...since we want our client's confidentiality to be respected in every possible way."*

We also learned that caseworkers discouraged clients from sharing their documents through communication tools such as *WhatsApp* or *Telegram*, regardless of whether they used their own mobile phones or borrowed devices from others, such as friends and family. Instead, clients were often advised to visit in person when necessary and to send documents electronically by email if required later. Our participants further informed us that most refugees already had email accounts by the time they met their caseworkers. These accounts had usually been created for them by volunteers while they were staying in immigration hotels, allowing them to access their UKVI portals. They were also given their login credentials, which most kept safe until they met their caseworkers. For those who had forgotten or lost their credentials, or who did not have an email account, as was the case for some asylum seekers, caseworkers created email accounts for them and took responsibility for keeping the credentials safe. These clients were then advised to access their email accounts from public libraries. Caseworkers would usually provide their clients with the locations of libraries offering public internet access. Some participating caseworkers mentioned that they provided specialised training to certain clients on how to stay safe online when responding to emails or sending documents by email. Most caseworkers reported that their clients, particularly refugees, had mobile phones or access to them. When clients did not have their own mobile phones, as was the case for most asylum seekers and some refugees, caseworkers advised them on how to use devices belonging to other people. This included guidance on responding to 2FA prompts when logging into their email accounts and avoiding saving email attachments on those devices. As one caseworker recalled, "*.....we don't get this a lot but there are clients who do not have anything neither cell phones or any kind of digital devices...while getting a new digital device for them becomes difficult...in case we hear them borrowing it from friends or family or using someone else's we try and provide them all the necessary advice about how to go about it safely...."*

4.1.3. Consent as a Fragile and Culturally Situated Process. Having access to client data, storing it on charity devices, and making legal or civic representations on clients' behalf meant that caseworkers needed to obtain their consent

4. https://www.charitylog.co.uk/

for these procedures. However, nearly all participants agreed that *"....understanding, explaining and receiving consent sometimes turned out to be a difficult task due to cultural reasons."* Some participants further commented that *"sometimes consent was assumed on the part of the client"* and that *"...making some of them understand the value and necessity of consent was often challenging.."* One caseworker recalled that, during an initial meeting, a client had found it *"surprising"* that they needed to give permission for the caseworker to contact the Home Office and respond to it on their behalf. This participant explained, *"....well you cannot think of them to know about all of this, especially if they are coming from a place where consent isn't crucial...you know GDPR and stuff... but it is our duty to make them understand we cannot do anything on their behalf unless they explicitly instruct us to do so"*.

The process of obtaining consent included three important steps. Firstly, caseworkers had to provide their clients with forms clearly stating what kind of data was being collected and stored and how it would be used to make representations to the Home Office on their behalf. The data collected at this stage included descriptions of their *personal journeys* and documents given to them by the Home Office. The next step was to explain each line of the form to clients and answer any questions they might have. During this process, interpreters who spoke the clients' languages were involved again. However, unlike during the initial narrative stage, friends and family were also permitted to assist with translating consent information, since the priority here was to ensure comprehension rather than preserve the originality of the client's account. The third step involved explaining UK GDPR regulations to clients, especially their right to withdraw consent if they felt it necessary. This was again taken care of by interpreters or friends and family, if needed.

The process of interacting with clients and obtaining their consent took place after clients had described their personal journeys to caseworkers, in the same enclosed space where they had first met and engaged with them. As our participants further explained, the consent forms were then stored securely in accordance with GDPR requirements. Importantly, participants declined to provide us with any further information about the secure storage of these forms during follow-up interviews, citing either "*organisational policy*" or "*client confidentiality*".

4.1.4. Home Office Correspondence and Downstream Circulation. Although caseworkers tried to protect client information, the UK Home Office repeatedly emerged in workshops and interviews as a source of *"messing up client confidentiality"*. Participants recounted instances of Home Office emails being sent to the wrong caseworkers, correspondence that *"asked for clarifications since they had mixed up people in their database,"* a specific instance in which the Home Office had *"lost two cabinets full of refugee and asylum seeker applications,"* and a UK Border Agency blunder in which *"they had destroyed close to fifty seven thousand landing cards citing data protection, automatically taking away people's ability to prove their lawful presence in the UK."* Caseworkers did not blame Home Office officials directly, attributing these errors to overburdened staff working under strict deadlines and metric-based targets. When breaches occurred, caseworkers took proactive steps by notifying the Home Office of misdirected correspondence and sometimes filing pre-protocol letters to ensure institutional accountability should a breach affect a client's application. The downstream consequences of these errors were significant. Confused or distressed clients, who received correspondence that did not pertain to them or unexpected rejection letters, turned to *"friends, family members and even unknown strangers"* for help, causing sensitive case information to circulate among people entirely outside their cases. Participants described clients *"going haywire, broken and at the brink of psychological collapse"* and highlighted how indiscriminate sharing led to extortion, exploitation and, in some cases, clients being drawn into situations of serious harm. As one participant explained, *"...when they get weird letters that ask them to explain things unrelated to them...they just throw themselves into a frenzy and then they are taken advantage of...female applicants sometime even fall prey into sex trafficking rackets as a result."*

4.1.5. Clients, AI, and the Problem of Premature Disclosure. Caseworker participants collectively expressed concern about their clients' use of conversational AI tools such as ChatGPT and how this compromised their privacy as a vulnerable group. One caseworker clarified: *"....it's not that all of them are absolutely destitute...some of them have cell phones regardless of their immigration status and some of them can borrow it from their friends or family...they can access ChatGPT easily in that case..."* Our participants raised two interrelated concerns. First, immigration narratives generated by AI chatbots often produced accounts that *"were unreal and sounded fabricated,"* making it difficult for caseworkers to accurately understand their clients' positions and potentially jeopardising their applications. Second, clients who entered personal information into AI chatbots risked what one participant called the *"problem of premature disclosure"*: their data could be stored, shared, or accessed by state actors, including the Home Office, at a stage when such disclosure could be damaging. As that participant summarised, *"AI chatbots only accentuated client desperation and made them commit certain actions that only risked their chances of getting their applications approved, or worse, leaked their personal information to establishments and institutions that should not have access to their data at that very moment."* These concerns were first raised during unstructured conversations and discussed in depth during the workshop. In subsequent interviews, we explored two follow-up questions. First, we asked how narratives crafted by LLMs differed from fabrications that clients might have produced independently. According to caseworkers with decades of experience, fabrication had previously been *"like 1/100."* The more pressing issue, they explained, was not the fabricated narrative itself but *"the psychological effect it had on the client."* Due to the sycophantic tendencies of language models, asylum seekers used AI-generated narra-

tives alongside existing statutes to justify their claims more forcefully. Our participants noted that these *"AI generated polished narratives would strip away even if there is an iota of honesty in their statements."* Clients who turned away from the charity armed with AI-reinforced beliefs became vulnerable to immigration fraud and labour exploitation. As one caseworker concluded, *"Previously these people would just listen to us and stop in most situations...but now they have a machine telling them go ahead and do it...."*

Second, we asked about the practical consequences of the Home Office or a similar actor gaining access to a client's LLM chat logs. Here, our participants' concerns centred on preconditioned bias and procedural fairness. A practising solicitor among our participants noted that the Home Office's use of AI agents in asylum adjudication had already been challenged in court for being *"unreasonable and inconclusive,"* and expressed concern that prior statistical information about clients could influence automated decisions against them. Another caseworker described how *"some clients while using AI inadvertently uploaded pictures of themselves, their passports and any travel document...and have conversations around them such as they would like to get rid of the passport when they can settle here."* Such conversations, if surfaced out of context, could result in unfair treatment during adjudication. As one caseworker warned, *"people or even officials may have a wrong and context-absent idea about these people simply wanting to settle in the UK because they want to travel the world visa free...there are bad people who'd love to hack and hunt these asylum seekers down."*

4.2. Organisational and Personal Security Risks Facing Caseworkers

4.2.1. Organisational Invisibility as a Security Strategy. Our field visits revealed that organisations sought to minimise their public visibility as much as possible, both at the organisational and individual levels. Two of the charities we visited were housed in buildings without signboards that would allow people outside to identify them easily. As one caseworker commented, *"...people who have to find us will definitely find us, but we [do] not want all people to know where we are located, especially in this political climate.."* Our participants attributed their low-profile mode of operation to rising political tensions across the UK and Europe directed against immigrants, with certain "new political actors" expressing disapproval of refugees and asylum seekers. Even within their offices, the names and pictures of trustees displayed on the walls were positioned discreetly, making them difficult to see from a distance. One participant explained that this was intended to ensure that, in the event of an unforeseen situation, such as *"a violent break-in by people who do not support immigration"*, trustees would not be specifically targeted. Elaborating on this, the caseworker remarked, *"...managements and trustees are usually the first people to get attacked from our previous experience, hence we have decided to keep things to a minimum."* Participants also pointed out that their respective charities maintained a minimal online presence, with very simple websites providing little information, and preferred not to share details of their work or operations on social media. As one participant explained, *"....there was once an incident where we received threats for running a charity that helps in immigration and since then we removed the pictures of our caseworkers from the website.."*

Caseworkers described their personal security strategies as part of their *"work ethic and professional discipline"*. This concern for safety was not only individual but also institutional. Participants noted that caseworkers were hired or permitted to work with clients only after passing Disclosure and Barring Service (DBS) checks, through which charities sought to protect organisational integrity, client safety, and trust in their services. Separately, most caseworkers avoided publicly identifying themselves as immigration caseworkers.

For example, one participant explained that they usually told people they were not formally employed and only volunteered at a local charity, without specifying the nature of the charity's work. When pressed to explain what the organisation did, including within family circles, they would *"make up something"* and describe it more generally as a charity that helped *"the poor and distressed"* or addressed homelessness. This caution also shaped how caseworkers managed communication with clients. Almost all participants avoided sharing their personal mobile numbers with clients. They preferred to communicate through appointments or walk-ins where possible, and received documents by email when necessary. One caseworker who used a personal phone acknowledged that this could be risky, noting that they sometimes received threats when clients received unfavourable decisions. However, they explained that they *"understood the momentary frustration"* and did not feel personally afraid, drawing on their own experiences of migration and insecurity. Participants also described maintaining low public profiles, with little to no social media presence, and avoiding meetings with new acquaintances unless they had been introduced through trusted sources, such as family members or long-term friends.

Participants also generally avoided using their personal phones for casework purposes. Charities that could not afford to provide caseworkers with mobile phones mostly relied on landlines paid for by the charity, with the numbers listed on their websites. These telephone connections were important because caseworkers often had to coordinate with other charities to arrange housing for asylum seekers and refugees or provide them with food. They highlighted that *"...often connecting with other organisations through your own cell phone could risk your number being leaked to not just clients but other ill-intentioned people"*. In this regard, one caseworker described how a local library had leaked their phone number after they contacted it on a client's behalf to arrange computer access.

4.2.2. Physical and Digital Security of Caseworkers. During our field visits, we observed that charities had invested in both electronic and physical security measures. These included industry-grade locks which, according to partici-

pants, were designed to withstand forced entry, fire damage, lock snapping, and lock picking. Closed-circuit television (CCTV) cameras were strategically placed in rooms where client interactions took place, in hallways, and in client waiting areas. When we enquired about these placements, the caseworker representing one of the charities explained: *"the cameras were placed keeping in mind the safety requirement of caseworkers...client interactions needed to be monitored because some of them might suddenly become hostile the footage was needed in case they had to be later identified should they physically injure our staff.."* All caseworkers confirmed that they would not continue to see clients who engaged in activities such as physical assault. Cameras were placed in hallways specifically to *"keep a track of when clients and visitors entered and exited."* Those in waiting areas were primarily used to monitor visitors and clients and to *"find out later if they are taking any pictures of trustees or other documents such as attendance sheets or visitor notebooks that were present in the waiting room....thing which could portray them to be suspicious."*

Although charities saw clients through walk-ins where possible, no caseworker spoke to visitors who were not asylum seekers or refugees until they had first been assessed by a non-caseworker positioned near the charities' front doors. These individuals, often referred to as *"support staff of caseworker charities"*, would usually look through the door's peephole before admitting a visitor or client. Clients would only be shown to the waiting area once the support staff had confirmed the purpose of their visit and deemed it satisfactory. In most cases, these staff members would ask visitors who were not seeking asylum to confirm whether they had an appointment. If they did not, *"they'd either refuse entry or ask them to wait outside until they could confirm from the management if they can be let in."*, as one participant explained. This was primarily done to prevent unwanted visitors who might intend to disrupt the charity's work from entering the premises, as several caseworkers recounted from their experience. Every visitor entering through the door, whether an asylum seeker or not, had to sign an attendance book kept in the waiting area, whose integrity was protected through the closed-circuit surveillance described above.

All caseworkers noted that their charities had a "special relationship" with local councils and nearby police stations. This ensured that law enforcement officials could be contacted immediately for a swift response if something went wrong or a security threat arose. As one participant explained: *".....those who come to us are all very traumatised people but sometimes things get out of control and they become violent...during those instances we have to call the cops as a last resort but we never almost do it. The more immediate reason of having their numbers on our speed dials is because we have faced threats in the past where people harbouring certain political sentiments have come and protested here....it is since then we have tried to be as low-key as possible."*

All participants reported that their respective organisations received a high volume of spam emails and suspicious phone calls, some of which bypassed existing anti-spam filters and required caseworkers to assess their authenticity themselves. During interviews, participants described emails impersonating the Home Office, local councils, and law enforcement agencies, as well as messages from people in other countries seeking advice on how to emigrate. They had developed informal heuristics for assessing these communications, learning from experience, for instance, that the Home Office would not send grammatically incorrect emails or call to request personal information about clients. Some participants also described independently learning to check the origins of suspicious emails using email-header verification tools. The category of communication that caused the most concern, however, was not phishing targeting clients but messages claiming that the organisation's own camera servers or digital infrastructure had been breached. Participants described receiving such emails occasionally. These felt qualitatively different from ordinary spam because they raised the possibility that the organisation's surveillance systems and client attendance records could be exposed. As participants explained during interviews, these threats were harder to dismiss and verify, and some organisations lacked the technical capacity to assess them confidently.

4.2.3. Organisational Capacity and the Limits of Secure Practice. Despite the robust privacy and security practices in place, our field visits identified security lapses that we brought to participants' attention during the workshops. These included client names and addresses visible in visitor books in waiting areas, old files and hard disks labelled with their contents left around caseworkers' workspaces, and handwritten notes left on desks. Caseworkers from every organisation acknowledged these lapses but contextualised them within their organisational practices. Old files and hard disks pertained to legacy cases that had already been digitised and uploaded to the cloud. They were retained solely for regulatory reasons and tracked through weekly inventory checks. No participants reported anything missing from these records.

Incident reporting varied considerably across organisations. In most, no formal protocol existed, and caseworkers described a pattern in which *"incidents whether data breaches or harassment by clients were usually discussed in weekly meetings or monthly meetings with trustees where suggestions about keeping safe were updated if needed and then circulated among staff members as conveyed as guidelines by word of mouth."* One organisation had a formal system in place, through which designated personnel drafted incident reports that were presented to trustees to inform decisions about additional security infrastructure. Technical incidents, such as data breaches or phishing, were handled by a dedicated IT staff member who conducted security audits. At the other organisations, IT support was mostly part-time and voluntary, covering system maintenance, connectivity, antivirus updates, and occasional guidance to staff on phishing and identity theft risks.

Participants at one organisation described an incident in which a caseworker left a flash drive containing client data

on a bus. The caseworker realised this upon getting off the bus, returned immediately, and recovered the drive. Following the incident, caseworkers at the organisation adopted a practice of not taking work home.

4.2.4. Doing Casework Safely With AI. None of our participants argued against the use of AI in casework. Instead, many described large language models as tools that could make aspects of their work more productive and efficient. At the time of the workshops and interviews, participants' awareness of AI tools was largely limited to ChatGPT and Claude. Few could name other systems, including Perplexity, Mistral, and Gemini, and none were aware of open-weight models or local deployment tools such as Ollama. The use of AI in casework was largely restricted to drafting and polishing letters for housing applications, responding to Home Office emails in a *"professional manner"*, and occasionally finding resources for specific clients through a targeted search approach that *"helped narrow down searches quickly.."* All participants were, however, aware of AI hallucinations, which is why they sometimes manually checked AI-retrieved search results when *"something appeared to be unusual."* As one caseworker explained, *"....we often have to look for very obscure pieces of information that will not just appear in a single google search....it might be a white paper that had appeared sometime ago and now we cannot find it any more...me and my colleagues have seen Claude perform these targeted searches very well and it is almost never incorrect..."* Participants were careful never to upload details about their clients or themselves to language model interfaces, including names, addresses, or other identifiable information. They also never used AI chatbots to summarise client case files, as most had found such summaries inadequate in some cases. They were particularly careful not to upload templates containing their organisations' letterheads to AI chatbots or ask the systems to draft letters directly onto them for specific purposes. None of the participants gave AI chatbots integrated access to other tools, such as Google Drive, or to their professional or personal email accounts.

4.3. Commitments and the Political Climate

Participants described an ideological commitment to the law as the basis of their work, linking it to the political climate surrounding immigration. Some caseworkers said that, in climates hostile to immigration, they wanted decisions to follow the law and remain independent of public sentiment against immigration. They also emphasised that they could not act in the interests of any party, whether people hostile to immigration or people seeking asylum. As one participant put it, *"you see we cannot act in interest of anyone...not people who harbour feelings of anti immigration and neither individuals who want to simply seek asylum for the right reasons...we work as per law and the law is what we want to follow...that is our ideological commitment."* This stance coexisted with the care participants described for their clients, was reflected in how they attributed Home Office errors to overburdened staff, and shaped the low profile their organisations maintained in a politically hostile climate.

4.4. Summary of Protective Strategies

Taken together, caseworkers' protective practices formed a layered response to risks arising at different points in casework. Some practices protected information during interactions with clients, including restricted consultations, interpreter use, and explained and documented consent. Others governed how information was handled once it had been recorded or shared through communication channels. These included password-protected storage, guidance on messaging applications and email access, keeping client work on organisational premises, and correcting errors in institutional correspondence. A third group of practices protected staff and premises through limited public visibility, separation of personal communications from work-related communications, and visitor screening. More recent practices addressed suspicious communications, alleged breaches, and AI tools that caseworkers had to evaluate without specialist support.

Table 1 maps each strategy to the risk it addresses and the labour it requires. We use the term *risk* in this table because the exposures caseworkers managed included routine administrative issues, such as misdirected correspondence and visitor records, as well as deliberate attempts to obtain information. Adversaries in the narrower technical sense accounted for only some of these risks.

The table shows that protection depended on recurring work. Caseworkers coordinated rooms and interpreters, explained consent repeatedly, supported clients with accounts and authentication, and manually checked suspicious messages. Some of this labour created additional exposure. Handling credentials on behalf of clients was itself a point of risk, while the visitor records and camera systems used to secure premises contained identifiable information that also needed to be protected. Most of this labour fell to individual caseworkers, and the support available to them varied across organisations.

5. Discussion

Our findings reveal two connected dimensions of privacy and security practice in immigration casework. First, caseworkers undertake protective work as part of their broader humanitarian responsibilities towards clients. Their practices of managing consent, restricting information disclosure, correcting institutional errors, and limiting organisational visibility reflect concerns about the consequences that exposure may have for people navigating immigration processes. Second, these practices operate within organisations where technical expertise, formal procedures, and resources are unevenly available. Caseworkers consequently assume responsibility for recognising and responding to risks that extend beyond their immediate control. We discuss these findings in relation to existing accounts of situated security and humanitarian care, examine the sources of risk and organisational constraints that shape protective practice, and

TABLE 1. PROTECTIVE STRATEGIES REPORTED OR OBSERVED IN IMMIGRATION CASEWORK AND THE LABOUR INVOLVED IN MAINTAINING THEM.

Protective strategy	Risk addressed	Labour and practical constraints
Conducting consultations in restricted spaces and using interpreters	Disclosure of sensitive personal histories to unauthorised individuals	Coordinating rooms, appointments, interpreters and access under space constraints
Digitising documents and storing records in password-protected systems	Unauthorised access to or accidental disclosure of client information	Scanning, filing, managing access and maintaining physical records
Explaining consent and documenting authorisation	Use or disclosure of information without adequate client understanding	Interpreting, explaining procedures repeatedly, answering questions and maintaining consent records
Discouraging personal messaging applications and supporting email access	Exposure of documents through uncontrolled communication channels and shared devices	Creating accounts, transferring credentials, explaining authentication and supporting clients with limited access to devices
Keeping client work on organisational premises	Loss or exposure of client material taken off premises, for example on removable storage	Completing casework on premises and forgoing work at home
Reporting and correcting institutional correspondence errors	Unintended disclosure, misinformation and further circulation of sensitive records	Investigating correspondence, communicating with authorities and helping distressed clients understand decisions
Limiting public visibility and separating personal communications	Harassment, unwanted identification and disclosure of staff contact information	Maintaining restricted profiles, managing contact boundaries and using organisational communication channels
Screening visitors and monitoring organisational premises	Unauthorised entry, confrontation and exposure of organisational information	Managing entry, maintaining records and administering surveillance systems that themselves contain sensitive information
Assessing suspicious communications and claimed breaches	Impersonation, information theft and possible compromise of organisational infrastructure	Manually checking communications, escalating concerns and obtaining technical assistance where available
Restricting AI inputs, integrations and generated materials	Disclosure of client information and reliance on inaccurate output	Assessing permissible inputs, reviewing outputs and maintaining boundaries around connected organisational systems

consider their implications for the security and privacy community, both for the design of technologies for people who protect others and for how researchers and partners engage with organisations that serve vulnerable groups.

5.1. Security as Humanitarian Care

Across our findings, privacy and security were closely connected to the humanitarian responsibilities caseworkers understood themselves to hold towards their clients. Participants described assisting people who had experienced displacement, conflict, and uncertainty, often supporting needs extending beyond immigration applications to housing, healthcare, and access to essential provisions (Section 4.1.1). These commitments were reflected in how caseworkers handled sensitive information. As documented in our findings on client information protection (Section 4.1.2), participants arranged private consultations, restricted access to personal narratives, used interpreters, and maintained procedures for storing and sharing documents. Their accounts of consent (Section 4.1.3) further illustrated the attention they gave to explaining institutional requirements to clients who might be unfamiliar with them. Such practices were informed by an understanding that the consequences of disclosure could extend beyond a loss of confidentiality to affect clients' ability to obtain assistance and navigate immigration procedures.

Dourish and Anderson established that privacy and security are embedded in collective rhetorics of risk, trust, morality, and identity rather than reducible to technical controls alone [50]. Building on this perspective, McClearn et al. examined how protection is assembled from heterogeneous and partial resources under conditions of failing governance and infrastructural scarcity, describing this process as patch work to security [11]. Jensen et al. similarly demonstrated how forced migrants navigating digital resettlement services negotiate privacy and security alongside pressing needs for institutional access and support [6]. These accounts provide important ways of understanding the practices observed in our study. Caseworkers relied on shared professional expectations, informal knowledge, available technologies, and organisational arrangements to protect information while sustaining the services clients required.

Our findings extend these accounts by examining how responsibilities towards clients influence the purposes and boundaries of protective action. Participants were responsible for information belonging to people whose immigration

circumstances could make errors, disclosure, and misinterpretation particularly consequential. Their responses to misdirected Home Office correspondence (Section 4.1.4) illustrate this relationship. Caseworkers sought clarification, reported errors, and supported clients distressed by unexpected communications because they were concerned about the consequences for applications and the further circulation of personal information. Importantly, participants generally attributed such errors to overburdened officials and administrative pressures rather than deliberate misconduct (Section 4.1.4). They also described established relationships with local councils and police that supported their work and organisational safety (Section 4.2.2). Participants viewed these processes as unreliable and consequential for clients, shaping security practices around managing institutional failure without presuming adversarial relationships with the institutions involved.

We describe this orientation towards security as humanitarian care. The concept draws attention to protective practices undertaken as part of an ongoing responsibility for the welfare of others. Security patchworking helps explain how caseworkers assemble protection from the resources available to them [11], while the social understanding of security provides a basis for examining the values and relationships that shape such decisions [6], [50]. Our findings show how these dimensions converge in immigration casework, where caseworkers must protect sensitive information while continuing to facilitate access to institutions on which clients depend. The humanitarian commitments participants expressed (Sections 4.1.1 and 4.3) help explain why they undertook protective work beyond immediate administrative requirements, including assisting clients with digital access, explaining consent, and responding to information errors.

These commitments also shaped how participants understood their own visibility. Our findings on organisational invisibility (Section 4.2.1) documented charities operating from discreet premises, limiting identifying information on their websites, and avoiding unnecessary disclosure of staff and trustee identities. Participants connected these measures to experiences of threats and concerns about political hostility surrounding immigration (Sections 4.2.1 and 4.3). Caseworkers similarly described restricting their public profiles and separating personal contact information from professional communication. These practices sought to protect staff and sustain the organisations through which clients received assistance. Hence, the political environment shaped participants' security decisions, alongside their organisational circumstances and experiences.

Recognising security as humanitarian care has implications for how protective work is understood within resource-constrained organisations. Prior research has shown that organisations serving marginalised populations frequently carry responsibilities exceeding their infrastructural capacity [3], that security practices may develop around perceived rather than formally measured risks [4], and that trusted individuals often assume responsibilities in the absence of established institutional guidance [37]. Our findings illustrate how such conditions operate in immigration casework. Participants developed protective routines because they regarded client confidentiality and staff safety as integral to their responsibilities (Sections 4.1.2, 4.2.1, and 4.3), yet these routines were not always supported by consistent procedures or technical expertise (Section 4.2.3). Sustaining this work therefore requires attention to the organisational arrangements through which knowledge, documentation, and responsibility are maintained [13], while recognising the commitments and relationships already informing caseworkers' practices.

5.2. Risk Sources and Organisational Constraints

The findings also allow us to distinguish the different sources of privacy and security risks encountered in immigration casework. The information requiring protection included clients' personal narratives, identity documents, immigration correspondence, consent records, account credentials, and organisational records containing information about staff and visitors (Sections 4.1.2, 4.1.3 and 4.2.2). In the technical sense of threat modelling, potential adversaries included individuals impersonating public authorities to obtain information, hostile visitors seeking to disrupt organisational activities, and individuals who might deliberately exploit sensitive material disclosed outside established casework relationships (Sections 4.1.4 and 4.2.2). Participants described suspicious communications, previous threats to organisations, and concerns about the exploitation of clients following the circulation of personal information (Sections 4.1.4, 4.2.1 and 4.2.2). These accounts identify relevant adversarial risks, although they do not establish that every suspected communication represented a genuine attempt at compromise.

Other risks emerged without evidence of malicious intent. Participants described errors in Home Office correspondence that could expose information or prompt distressed clients to seek assistance from uninvolved third parties (Section 4.1.4). Clients using borrowed devices and public computers also faced circumstances in which their information could become accessible outside their control (Section 4.1.2). Similarly, visitor books and CCTV systems maintained for organisational safety created records containing identifiable information (Sections 4.2.2 and 4.2.3). These examples indicate that exposure could arise through ordinary administrative processes and protective infrastructures, as well as through deliberate attempts to obtain information. This distinction matters because the appropriate response to impersonation differs from the measures needed to correct institutional correspondence or support a client unfamiliar with shared-device security.

The practices developed in response to these risks depended substantially on caseworkers' judgement and organisational knowledge. Our findings on physical and digital security (Section 4.2.2) documented how participants identified suspicious messages through their experience with official correspondence, with some independently learning to inspect email headers. However, messages alleging breaches of organisational camera servers were particularly

difficult to assess, especially where technical expertise was unavailable. Similarly, while participants described restrictions on sharing client information through external AI systems (Section 4.2.4), these boundaries were largely maintained through individual decisions about appropriate use. Organisational arrangements provided some support through password-protected records, access controls, surveillance, and established communication channels (Sections 4.1.2 and 4.2.2), but they did not consistently address the circumstances in which caseworkers needed specialist assistance.

These limitations connect with wider concerns in human-centred security research. Prior work has shown how security responsibilities in nonprofit settings can become concentrated among individuals when organisational guidance and resources are limited [37]. Nonprofits also face competing demands from immediate service delivery and external accountability requirements, which can constrain investment in organisational infrastructure [27]. Humanitarian organisations face related pressures because they must remain accessible to people seeking assistance while protecting sensitive beneficiary information [43]. Our findings illustrate how these conditions affected immigration caseworkers, whose responsibilities included interpreting institutional correspondence, helping clients use digital services, protecting information, and responding to threats despite uneven access to technical support (Sections 4.1.2, 4.1.4 and 4.2.3).

The implication is that security knowledge needs to be sustained beyond individual caseworkers. In our study, caseworkers had developed ways of recording consent, storing information, limiting personal exposure, assessing communications, and responding to incidents (Sections 4.1.2, 4.1.3, 4.2.1, 4.2.2 and 4.2.3). However, organisational capacity to document and share these practices varied. Some incidents were discussed informally during staff or trustee meetings, while other organisations maintained more structured reporting arrangements and dedicated technical support (Section 4.2.3). Staff transitions and differences in technical familiarity could therefore affect the consistency with which these practices were maintained. Research on humanitarian organisations has argued that they need to build capacity continuously rather than rely on isolated technical interventions [43]. The implications for the security and privacy community are explored in the next subsection.

5.3. Implications for the Security and Privacy Community

Our findings describe people who protect vulnerable others while operating under threats of their own. Caseworkers support clients whose circumstances make exposure consequential, and they work in organisations whose premises, staff, and public profile attract hostility (Sections 4.2.1 and 4.2.2). Several contextual risk factors identified in research on at-risk users apply to them, including access to a sensitive resource, in this case, client information (Section 4.1.2) [20]. Protective work in this setting therefore serves two groups at once, and the integrity of casework depends on protecting both. This duality shapes what the security and privacy community owes these users in two respects. The first concerns the technologies they use, which need to be designed with the stakes of their work in mind. The second concerns how researchers, universities, and technical partners engage with organisations that are themselves under strain while serving vulnerable groups.

5.3.1. Designing to Preserve the Integrity of High-Stakes Work. Much of the technology caseworkers rely on assumes that users will work out its security implications for themselves. Security research has long noted that threat models and design defaults tend to centre the average user, leaving those with elevated exposure to improvise [20]. Our participants improvised effectively, drawing on experience, habit, and informal exchange, while their boundaries around AI tools, shared devices, and camera systems rested largely on individual judgement (Sections 4.1.2, 4.2.2 and 4.2.4). For people whose mistakes can expose a client or compromise an organisation, leaving security implications unstated carries a cost that current designs do not acknowledge.

We therefore argue for explanatory design that tells users, at the point of use, what a technology implies for the people whose information they hold. Field evidence shows that well-designed warnings change behaviour and that communicating security information to end users remains worthwhile [51]. Explainable Security proposes communicating experts' analyses of a system to varied audiences [52], while research on privacy notices shows that timing, channel, and modality shape whether notices are noticed and understood [53]. Existing approaches have concentrated on raising awareness of how systems behave. For populations whose work depends on protecting others, a more useful explanation concerns what using a technology means for that work. It should be delivered in a calm register that supports confident practice and vary sufficiently to resist the habituation that erodes the effectiveness of repeated warnings [54].

Three technologies in our findings illustrate what this could look like. Language model platforms typically warn that outputs may contain mistakes, yet caseworkers' central concern was the disclosure of client information to an external system (Sections 4.1.5 and 4.2.4). Studies of users of LLM-based agents have found erroneous mental models, design patterns that limit awareness of privacy risks, and human-like interaction that encourages sensitive disclosure [55]. Research on AI used in homeless services has likewise examined the perspectives of frontline workers and the people they serve [56]. Providers of language model platforms could state plainly, at the point of text entry, that sharing personal details about the user or others could cause prejudice or jeopardise the user's work. Operating system vendors could pair the safe-ejection prompt for removable storage with a reminder to keep the device secure. In one organisation, a caseworker left a flash drive containing client data on a bus and recovered it after realising this upon getting off. Caseworkers in that organisation subsequently stopped taking work home (Section 4.2.3). Experimental

work finds that people who come across an unattended drive frequently plug it in and open its files [57], so a drive that is not recovered carries the risk of disclosure. CCTV systems installed for organisational safety record staff, clients, and visitors in settings where being identified can be risky (Section 4.2.2). Regulatory guidance already expects people to be informed that they are being recorded, with signage placed before the entrance to the camera's field of view [58]. Suppliers and installers could prompt immigration charities to meet that expectation discreetly and explain how footage is stored, where it travels, and who can access it.

5.3.2. Engagement, Capacity Building, and the Risk of Extractive Partnership. A further implication concerns how the security and privacy community engages with organisations that serve vulnerable groups while facing risks of their own. Researchers and technical partners who approach such organisations ask them to share information about clients, practices, and incidents that is sensitive to both the organisations and the people they serve. Research involving at-risk users presents safety challenges for both participants and researchers, and the community has begun to develop shared practices for addressing these challenges [59]. Reviews of privacy research with marginalised groups report that important methodological choices often go unreported and call for shared best practices [19], while calls for inclusive privacy and security urge the community to serve people with varied characteristics, abilities, needs, and values [60]. Our findings highlight a setting in which the organisation being approached is itself under strain, such that the way engagement is conducted can strengthen or undermine the protective work already underway.

Capacity building in this setting should begin with the knowledge and routines that caseworkers already use. Workshops with immigration support organisations could provide opportunities to share and compare approaches to document handling, communication, incident reporting, and AI use. Such activities would be particularly relevant where organisations had encountered similar problems but developed different responses because of staffing or financial constraints. They could also support discussions of situations that participants found difficult to assess individually, including institutional impersonation, alleged infrastructure breaches, and requests for sensitive information (Section 4.2.2). The purpose would be to make existing protective knowledge available across organisational roles and establish clearer responsibilities for responding to unfamiliar incidents [43].

Universities and nonprofit organisations with relevant technical expertise could act as **facilitators of collective learning**, particularly where charities could not independently resource sustained security support. Clinical models offer one precedent: trained consultants help victims of intimate partner violence secure their devices and accounts in coordination with support organisations [22]. Community studybeds developed with third-sector organisations in the UK treat partners as co-researchers who shape the focus, pace, and dissemination of the work and receive benefits in return [61]. Earlier participatory security research has also emphasised the importance of working at a pace that suits participants [62].

However, external involvement raises questions about access to organisational information and the purposes for which knowledge obtained through collaboration may be used. This concern is particularly relevant in immigration contexts, where information about clients and organisational practices may be sensitive beyond its immediate administrative purpose. Research on digital technologies in migration governance has raised concerns about data collection and the limited control available to people affected by these systems [63]. Participatory approaches also carry risks, as community-based engagement can reproduce privilege and cause unintentional harm when it involves collecting detailed personal narratives [64]. Collaborations intended to strengthen security should therefore consider whether their own information requirements could create additional risks of exposure.

For this reason, capacity building should take the form of accountable partnerships in which participating organisations retain authority over the information shared and the outcomes produced. Although nonprofit actors such as universities may have opportunities to provide support outside commercial service arrangements [24], their institutional position does not itself guarantee that collaboration will meet caseworkers' needs. Agreements should clarify the information required, the purposes for which it will be used, the access granted to external participants, and the resources or knowledge that will remain with the organisation. Additionally, partners should work with each organisation to define what vulnerability means in its own context, recognising that its meaning may differ across organisations serving similar groups [61]. These considerations follow from the confidentiality practices and organisational constraints documented in our findings (Sections 4.1.2 and 4.2.3) and provide a basis for ensuring that external assistance supports existing protective responsibilities.

6. Conclusion

This study examined how privacy and security are negotiated in the everyday work of immigration caseworkers in England. Our findings show that security in this setting is sustained by humanitarian care, a commitment to lawful and impartial processes, and professional judgement, with limited support from formal training or technical infrastructure. Caseworkers interpret documents, manage consent, limit disclosure, and protect their own visibility because they understand that clients' ability to be believed, represented, and supported depends on how their information is handled. This orientation gives security practices a specific form and urgency that existing frameworks of situated and usable security do not fully account for. The structural gaps documented in this paper arise from this condition: organisations whose security practices depend more on commitment and judgement than on formal resourcing face a persistent mismatch between the sensitivity of the information they hold and the infrastructure available to protect it. Addressing

this requires shared organisational infrastructure developed through partnerships that are accountable to the humanitarian orientation they aim to strengthen. As AI systems become more embedded in immigration governance, these questions become increasingly urgent for HCI and usable security research.

6.1. Limitations and Future Work

Our study was conducted with three migrant support organisations across different regions of England, and the findings reflect the conditions, practices, and pressures of this specific context. The workshop brought all twenty-one participants together in a single collective session, and it is possible that inter-organisational dynamics or differences in seniority shaped what caseworkers felt comfortable raising in that setting. However, the subsequent individual interviews provided an opportunity for participants to revisit and expand on issues they may not have raised collectively. Organisations operating in other parts of the UK or in different national settings may face meaningfully different infrastructural, legal, and political conditions that shape security practices in ways our study does not capture. Within England, the organisations we studied served client populations drawn predominantly from particular regions of origin, and the privacy and security dynamics that emerged from our fieldwork may not fully reflect the experiences of caseworkers supporting clients from different backgrounds, legal routes, or immigration histories. Future work should extend this inquiry to a broader range of organisations and client populations, attending to how the origins, legal statuses, and circumstances of the people being served shape the privacy and security demands placed on caseworkers and the organisations they work for.

Acknowledgements

We thank all participants for their time and valuable contributions. We also appreciate the constructive feedback from the anonymous IEEE S&P reviewers and our shepherd, which helped improve the clarity and presentation of our work. Arshia Dutta's research is supported by UKRI through the Centre for Doctoral Training in Cyber Security for the Everyday at Royal Holloway, University of London (EP/S021817/1).

References

[1] D. James and E. Killick, "Empathy and expertise: Case workers and immigration/asylum applicants in london," *Law & Social Inquiry*, vol. 37, no. 02, p. 430–455, 2012.

[2] A. Dutta and R. Bjerg Jensen, "Security at the border? the lived experiences of refugees and asylum seekers in the uk," in *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI '26, (New York, NY, USA), Association for Computing Machinery, 2026.

[3] A. F. Luo, N. Warford, S. Dooley, R. Greenstadt, M. L. Mazurek, and N. McDonald, "How library IT staff navigate privacy and security challenges and responsibilities," in *32nd USENIX Security Symposium (USENIX Security 23)*, (Anaheim, CA), pp. 5647–5664, USENIX Association, Aug. 2023.

[4] N. McDonald, B. M. Hill, R. Greenstadt, and A. Forte, "Privacy, anonymity, and perceived risk in open collaboration: A study of service providers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, (New York, NY, USA), p. 1–12, Association for Computing Machinery, 2019.

[5] S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer, "Usability analysis of shared device ecosystem security: informing support for survivors of iot-facilitated tech-abuse," in *Proceedings of the New Security Paradigms Workshop*, NSPW '19, (New York, NY, USA), p. 1–15, Association for Computing Machinery, 2020.

[6] R. B. Jensen, L. Coles-Kemp, and R. Talhouk, "When the civic turn turns digital: Designing safe and secure refugee resettlement," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, p. 1–14, ACM, Apr. 2020.

[7] D. Sabie, C. Ekmekcioglu, and S. I. Ahmed, "A decade of international migration research in hci: Overview, challenges, ethics, impact, and future directions," *ACM Trans. Comput.-Hum. Interact.*, vol. 29, Mar. 2022.

[8] S. He, X. Zhan, Y. Lei, Y. Liu, R. Abu-Salma, and J. Such, "Exploring the privacy and security challenges faced by migrant domestic workers in chinese smart homes," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, p. 1–18, ACM, Apr. 2025.

[9] S. He, Y. Lei, X. Zhan, R. Abu-Salma, and J. Such, ""these cameras are just like the eye of sauron": A sociotechnical threat model for ai-driven smart home devices as perceived by uk-based domestic workers," 2026.

[10] J. Slupska, S. Cho, M. Begonia, R. Abu-Salma, N. Prakash, and M. Balakrishnan, ""they look at vulnerability and use that to abuse you'': Participatory threat modelling with migrant domestic workers," in *31st USENIX Security Symposium (USENIX Security 22)*, (Boston, MA), pp. 323–340, USENIX Association, Aug. 2022.

[11] J. McClearn, R. B. Jensen, and R. Talhouk, "Othered, silenced and scapegoated: Understanding the situated security of marginalised populations in lebanon," in *32nd USENIX Security Symposium (USENIX Security 23)*, (Anaheim, CA), pp. 4625–4642, USENIX Association, Aug. 2023.

[12] J. McClearn, R. B. Jensen, and R. Talhouk, "Security patchworking in lebanon: Infrastructuring across failing infrastructures," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, Apr. 2024.

[13] J. Slupska and A. Strohmayer, "Networks of care: Tech abuse advocates' digital security practices," in *31st USENIX Security Symposium (USENIX Security 22)*, (Boston, MA), pp. 341–358, USENIX Association, Aug. 2022.

[14] C. Chen, N. Dell, and F. Roesner, "Computer security and privacy in the interactions between victim service providers and human trafficking survivors," in *28th USENIX Security Symposium (USENIX Security 19)*, (Santa Clara, CA), pp. 89–104, USENIX Association, Aug. 2019.

[15] Y. Zou, A. McDonald, J. Narakornpichit, N. Dell, T. Ristenpart, K. Roundy, F. Schaub, and A. Tamersoy, "The role of computer security customer support in helping survivors of intimate partner violence," in *30th USENIX Security Symposium (USENIX Security 21)*, pp. 429–446, USENIX Association, Aug. 2021.

[16] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno, "Computer security and privacy for refugees in the united states," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 409–423, 2018.

[17] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub, "Keeping a low profile? technology, risk and privacy among undocumented immigrants," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, (New York, NY, USA), p. 1–15, Association for Computing Machinery, 2018.

[18] M. Tran, C. W. Munyendo, H. Sri Ramulu, R. G. Rodriguez, L. Ball Schnell, C. Sula, L. Simko, and Y. Acar, "Security, privacy, and data-sharing trade-offs when moving to the united states: Insights from a qualitative study," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 617–634, 2024.

[19] S. Sannon and A. Forte, "Privacy research with marginalized groups: What we know, what's needed, and what's next," *Proc. ACM Hum.-Comput. Interact.*, vol. 6, Nov. 2022.

[20] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. G. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas, "Sok: A framework for unifying at-risk user research," in *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 2344–2360, 2022.

[21] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo, "Stories from survivors: Privacy & security practices when coping with intimate partner abuse," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, (New York, NY, USA), p. 2189–2201, Association for Computing Machinery, 2017.

[22] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart, "Clinical computer security for victims of intimate partner violence," in *Proceedings of the 28th USENIX Conference on Security Symposium*, SEC'19, (USA), p. 105–122, USENIX Association, 2019.

[23] D. Freed, S. Havron, E. Tseng, A. Gallardo, R. Chatterjee, T. Ristenpart, and N. Dell, ""is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, Nov. 2019.

[24] E. Tseng, M. Sabet, R. Bellini, H. K. Sodhi, T. Ristenpart, and N. Dell, "Care infrastructures for digital security in intimate partner violence," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, (New York, NY, USA), Association for Computing Machinery, 2022.

[25] S. L. Star and A. Strauss, *Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work*, p. 351–374. The MIT Press, Feb. 2016.

[26] Y. Sun, X. Ma, S. Lindtner, and L. He, "Data work of frontline care workers: Practices, problems, and opportunities in the context of data-driven long-term care," *Proc. ACM Hum.-Comput. Interact.*, vol. 7, Apr. 2023.

[27] C. Bopp, E. Harmon, and A. Voida, "Disempowered by data: Nonprofits, social enterprises, and the consequences of data-driven work," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, (New York, NY, USA), p. 3608–3619, Association for Computing Machinery, 2017.

[28] A. Voida, E. Harmon, and B. Al-Ani, "Homebrew databases: complexities of everyday information management in nonprofit organizations," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, (New York, NY, USA), p. 915–924, Association for Computing Machinery, 2011.

[29] L. Dombrowski, G. R. Hayes, M. Mazmanian, and A. Voida, "E-government intermediaries and the challenges of access and trust," *ACM Trans. Comput.-Hum. Interact.*, vol. 21, Feb. 2014.

[30] S. Erete, E. Ryou, G. Smith, K. M. Fassett, and S. Duda, "Storytelling with data: Examining the use of data by non-profit organizations," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, (New York, NY, USA), p. 1273–1283, Association for Computing Machinery, 2016.

[31] A. Voida, E. Harmon, and B. Al-Ani, "Bridging between organizations and the public: volunteer coordinators' uneasy relationship with social computing," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, (New York, NY, USA), p. 1967–1976, Association for Computing Machinery, 2012.

[32] S. Chowdhary, A. Kawakami, M. L. Gray, J. Suh, A. Olteanu, and K. Saha, "Can workers meaningfully consent to workplace wellbeing technologies?," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '23, (New York, NY, USA), p. 569–582, Association for Computing Machinery, 2023.

[33] D. Saxena, K. Badillo-Urquiola, P. J. Wisniewski, and S. Guha, "A framework of high-stakes algorithmic decision-making for the public sector developed through a case study of child-welfare," *Proc. ACM Hum.-Comput. Interact.*, vol. 5, Oct. 2021.

[34] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, (New York, NY, USA), Association for Computing Machinery, 2012.

[35] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," *Journal of Cybersecurity*, p. tyv008, Dec. 2015.

[36] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, (USA), p. 309–325, USENIX Association, 2015.

[37] N. Nthala and I. Flechais, "Informal support networks: an investigation into home data security practices," in *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS '18, (USA), p. 63–82, USENIX Association, 2018.

[38] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, (New York, NY, USA), Association for Computing Machinery, 2010.

[39] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How i learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, (New York, NY, USA), p. 666–677, Association for Computing Machinery, 2016.

[40] R. Wash, N. Nthala, and E. Rader, "Knowledge and capabilities that non-expert users bring to phishing detection," in *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security*, SOUPS'21, (USA), USENIX Association, 2021.

[41] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," in *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, (USA), p. 399–414, USENIX Association, 2015.

[42] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. Von Landesberger, and M. Volkamer, "An investigation of phishing awareness and education over time: when and how to best remind users," in *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, SOUPS'20, (USA), USENIX Association, 2020.

[43] S. Le Blond, A. Cuevas, J. R. Troncoso-Pastoriza, P. Jovanovic, B. Ford, and J.-P. Hubaux, "On enforcing the digital immunity of a large humanitarian organization," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 424–440, 2018.

[44] R. S. Chauhan, "Unstructured interviews: are they really all that bad?," *Human Resource Development International*, vol. 25, p. 474–487, Apr. 2019.

[45] R. Talhouk, L. Coles-Kemp, R. B. Jensen, M. Balaam, A. Garbett, H. Ghattas, V. Araujo-Soares, B. Ahmad, and K. Montague, "Food aid technology: The experience of a syrian refugee community in coping with food insecurity," *Proc. ACM Hum.-Comput. Interact.*, vol. 4, Oct. 2020.

[46] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, p. 77–101, Jan. 2006.

[47] V. Braun and V. Clarke, "To saturate or not to saturate? questioning data saturation as a useful concept for thematic analysis and sample-size rationales," *Qualitative Research in Sport, Exercise and Health*, vol. 13, p. 201–216, Dec. 2019.

[48] K. Vasileiou, J. Barnett, S. Thorpe, and T. Young, "Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period," *BMC Medical Research Methodology*, vol. 18, Nov. 2018.

[49] J. Ritchie and J. Lewis, eds., *Qualitative research practice*. Thousand Oaks, CA: SAGE Publications, Feb. 2003.

[50] P. Dourish and K. Anderson, "Collective information practice: Exploring privacy and security as social and cultural phenomena," *Human-Computer Interaction*, vol. 21, no. 3, p. 319–342, 2006.

[51] D. Akhawe and A. P. Felt, "Alice in warningland: A Large-Scale field study of browser security warning effectiveness," in *22nd USENIX Security Symposium (USENIX Security 13)*, (Washington, D.C.), pp. 257–272, USENIX Association, Aug. 2013.

[52] L. Viganò and D. Magazzeni, "Explainable security," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 293–300, 2020.

[53] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, (Ottawa), pp. 1–17, USENIX Association, July 2015.

[54] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance, "How polymorphic warnings reduce habituation in the brain: Insights from an fmri study," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, (New York, NY, USA), p. 2883–2892, Association for Computing Machinery, 2015.

[55] Z. Zhang, M. Jia, H.-P. H. Lee, B. Yao, S. Das, A. Lerner, D. Wang, and T. Li, ""it's a fair game", or is it? examining how users navigate disclosure risks and benefits when using llm-based conversational agents," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, (New York, NY, USA), Association for Computing Machinery, 2024.

[56] T.-S. Kuo, H. Shen, J. Geum, N. Jones, J. I. Hong, H. Zhu, and K. Holstein, "Understanding frontline workers' and unhoused individuals' perspectives on ai used in homeless services," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, (New York, NY, USA), Association for Computing Machinery, 2023.

[57] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey, "Users really do plug in usb drives they find," in *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 306–319, 2016.

[58] Information Commissioner's Office, "Video surveillance (including guidance for organisations using CCTV)." ICO guidance for organisations, 2022. Accessed 4 October 2026.

[59] R. Bellini, E. Tseng, N. Warford, A. Daffalla, T. Matthews, S. Consolvo, J. P. Woelfer, P. Gage Kelley, M. L. Mazurek, D. Cuomo, N. Dell, and T. Ristenpart, "Sok: Safer digital-safety research involving at-risk users," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 635–654, 2024.

[60] Y. Wang, "The third wave? inclusive privacy and security," in *Proceedings of the 2017 New Security Paradigms Workshop*, NSPW '17, (New York, NY, USA), p. 122–130, Association for Computing Machinery, 2017.

[61] K. M. Ramokapane, L. Coles-Kemp, N. Patnaik, R. Huan, N. Ajmeri, G. Liveley, and A. Rashid, "Towards equitable privacy," 2023.

[62] L. Coles-Kemp, A. Angus, and F. Stang, "Letting go: working with the rhythm of participants," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '13, (New York, NY, USA), p. 373–378, Association for Computing Machinery, 2013.

[63] Amnesty International, "Global: New technology and ai used at borders increases inequalities and undermines human rights of migrants." News, May 2024. Accessed 18 May 2026.

[64] C. Harrington, S. Erete, and A. M. Piper, "Deconstructing community-based collaborative design: Towards more equitable participatory design engagements," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, Nov. 2019.

Appendix A. Ethical Considerations

This study received institutional ethical approval, and the study objectives were clearly communicated to all participants prior to data collection and analysis. Participation was voluntary, and informed consent was obtained from all participants. Given the sensitivity of the material discussed, interviews were documented through detailed contemporaneous notes rather than audio recordings, minimising the volume of identifiable data held by the research team and affording participants greater control over what was captured. All data was handled in accordance with UK GDPR requirements. Organisational access was built through sustained engagement rather than extractive data collection, and participants were free to pause, redirect, or withdraw at any point during the study. There is no public link between our research team, which volunteered to conduct this research, and the organisations that participated in the study. The organisations' own volunteering bylaws require volunteers not to disclose their affiliation with the organisations, and this requirement has been consistently respected. This relationship is not disclosed in any professional profile, publication, or public material associated with the researchers.

Appendix B. Meta-Review

The following meta-review was prepared by the 2027 IEEE Symposium on Security and Privacy (S&P) Programme Committee, in accordance with the review process outlined in the Call for Papers.

B.1. Summary

This paper presents a study of the security considerations of immigration caseworkers in England. The authors conducted field observations, workshops, and interviews with caseworkers at 3 different migrant support organizations to investigate the security and privacy risks the caseworkers encounter in their work, and the risks they face personally. The analysis highlights that security and privacy challenges are intertwined with daily work. Security gaps result from lack of resources and lack of formal policy and robust technical guidance.

B.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field

B.3. Reasons for Acceptance

1) This paper addresses an important and understudied population whose work raises unique S&P challenges. The paper does an excellent job situating the work within prior HCI and S&P research while

clearly articulating why immigration caseworkers occupy an interesting intersection between these areas.

2) The methods were well-suited to the research questions, and the authors demonstrated thought and care in the study design. This consideration is particularly important given the sensitivity of the participant population and strengthens the overall study.
3) The combination of interviews, site visits, and a workshop provides a rich perspective on the work practices of migrant caseworkers and results in an informative characterization of their security and privacy challenges.