

# Security, Privacy, and Data-sharing Trade-offs When Moving to the United States: Insights from a Qualitative Study

Mindy Tran<sup>\*†§</sup>, Collins W. Munyendo<sup>\*§</sup>, Harshini Sri Ramulu<sup>\*†§</sup>, Rachel Gonzalez Rodriguez<sup>\*</sup>,  
Luisa Ball Schnell<sup>\*</sup>, Cora Sula<sup>\*</sup>, Lucy Simko<sup>\*</sup>, and Yasemin Acar<sup>\*†</sup>

<sup>\*</sup> The George Washington University, USA

<sup>†</sup> Paderborn University, Germany

**Abstract**— Moving to a new country often means that people leave their “known environment” and interact with new entities, often sharing sensitive and personal information. This exposes them to various risks. In this study, we investigate the challenges and concerns related to security, privacy, and data-sharing for people who have recently moved to the United States. Through semi-structured interviews ( $n = 25$ ), we find that most participants feel uncomfortable sharing documents containing their personal and sensitive information for the visa process e.g., their financial information and proof of relationship. Sharing this information makes participants concerned about their safety and privacy and sometimes violates their cultural information-sharing norms. Moving to a new environment, particularly to the US, also makes people vulnerable to fraud, specifically fraudulent online renting posts and scam calls. Those who move also navigate bureaucratic, administrative, and technical challenges that exacerbate their perceived security and privacy concerns. We further find a power imbalance that compels visa applicants to share all required information—to avoid getting their visa rejected—without feeling fully informed about the requirements and safeguards in place. Our study highlights the need for more guidance, transparency, and respect for individuals’ privacy from embassies and for technology designers to better support and protect those moving countries.

## 1. Introduction

Every year, many people move to new countries seeking employment, education, or even to escape conflicts. The United States (US) is a popular destination for many people moving and has outright the highest number of immigrants in the world, with a reported 44.8 million immigrants as of 2018, accounting for a fifth of the world’s total immigrants, and 13.7% of the US population [6].

However, moving to a new country—especially to the US—requires individuals to provide substantial personal information to acquire a visa, and then navigate new bureaucracies with newly assigned personal information, e.g., a social security number. Prior research has shown that refugees—a subset of immigrants—may find the influx of

new information confusing, and the advice around sharing information contradictory, leading to security and privacy challenges [50]. Additionally, the process of acquiring a US visa requires significant personal information, time, and paperwork from applicants, and is often invasive and lengthy. Indeed, there are inherent tensions between *national security* and *personal security and privacy* (and feelings of violation) during the visa process due to the substantial acquisition of visa applicants’ personal information. Additionally, the visa process may be intended as a deterrent for applicants from certain countries and visa types, perhaps more than others.

In this paper, we investigate the intertwined roles of information, security, privacy, and safety through the process of obtaining a visa and moving to the US. We explore how the visa process can violate cultural information-sharing norms and how power imbalances compel applicants to share documents and information without resolving privacy concerns. We examine applicants’ views of the process itself as well as how ambiguities and miscommunications create confusion for applicants, making them vulnerable to scams. We additionally explore participants’ sources of concern during the visa process, the aspects of the process they find acceptable, and reasons for this. Beyond the visa process, we explore technical security and privacy issues that arise due to new geographical restrictions, such as geo-filtering, once participants have moved, as well as their vulnerability to scams and administrative issues once in the US. Additionally, we investigate participants’ sources of advice and its impact on their digital security and privacy. More specifically, we seek to address the following five research questions:

- RQ1:** What threats, risks, and concerns, especially to personal information and documents, do participants moving to the US perceive during the visa process?
- RQ2:** What scams and other adverse experiences do participants encounter throughout the process of moving?
- RQ3:** What bureaucratic and administrative challenges through the visa process do participants encounter and how do they impact their security and privacy?
- RQ4:** What technical security, privacy, and access challenges do participants face due to moving to the US?
- RQ5:** What are participants’ sources of security and privacy advice throughout the moving process and how does this impact their digital security and privacy?

§. Co-first authors; please cite as Tran, Munyendo, and Ramulu et al. Since they all contributed equally to this work, the co-first authors may prioritize their names when adding this paper’s reference to their own CVs.

To answer our research questions, we conducted semi-structured interviews ( $n = 25$ ) with participants who had recently moved to the US from 17 different countries. We recruited participants first from personal contacts, followed by social media and online recruitment portals such as Prolific. We conducted the interviews remotely via Zoom between July and September 2022 and asked participants to detail information they had to share both prior to and after moving, the entities and channels through which they had to share this information, any concerns they had, as well as challenges in the moving process. We also asked participants about their sources of advice, particularly relating to security and privacy, during the moving process, and any adverse experiences they encountered, such as scams.

Overall, our main findings are summarized as follows:

**The US visa process requires substantial personal information and documents including financial and medical records that make applicants feel concerned about their security and privacy.** Our interviews reveal that participants are required to share several documents containing personal and sensitive information of themselves and their family members, that makes them concerned about their personal safety and privacy. For example, some participants were worried that leakage of their families' financial information may make them targets for robbery or extortion. Those applying for spouse visas had to provide proof of their relationships for example through wedding photos or private conversations with their partners which often made them uncomfortable and violated their cultural information-sharing norms. At the same time, participants felt compelled to share this information to avoid getting their visa rejected.

**Bureaucratic and administrative processes exacerbate perceived security and privacy risks.** As part of the visa process, applicants struggled with unclear and missing information on embassy websites as well as a general lack of assistance from embassies, leading some to share sensitive information with third parties when seeking help. Some participants were also concerned about the lack of physical privacy during visa interviews, which further amplified risks to participants' and their families' safety.

**People's unfamiliarity with their new environment after moving makes them vulnerable to scams.** While none of the participants in our study fell for any scams prior or during their move, several participants were concerned about rental scams as they had to rent an apartment in the US before moving. After moving, participants were targeted with scam calls and phishing messages, with some participants inadvertently sharing their personal information with illegitimate entities. One participant had to close their bank account after giving away their banking information.

**People encounter technical security, privacy and access challenges due to their move to the US.** As a result of moving to the US, participants struggled to access websites and content from their home country, either due to

geo-filtering or challenges with multi-factor authentication because of their previous telephone numbers being out of service. Some participants struggled to download apps, as their phones still had app stores of their home countries.

**Those who move countries may prioritize general advice about moving over security and privacy advice.** Due to insufficient support from embassies, most participants turned to friends and their family for advice, especially regarding the visa and moving process. Despite the substantial information that applicants had to share for the visa process, security and privacy advice was limited or less sought.

Overall, the perceived threats and risks, as well as participants' lived experiences and vulnerability throughout the moving process, suggest the need for better support for individuals moving from various stakeholders. We argue for more guidance, transparency, and respect for participants' privacy from embassies, including holding visa interviews in closed spaces as well as limiting personal information collected from applicants. Moreover, technology designers should re-evaluate the implications of their design decisions on specific populations, particularly with regards to geo-filtering and multi-factor authentication on those moving.

## 2. Background

When traveling or moving to a foreign country for a long duration, most people have to first obtain a visa authorizing their travel. Visas are typically issued by the consulate or embassy of the foreign country from the applicant's home country, and are normally stamped on the traveler's passport. In this section, we provide a broad overview of the visa application process for individuals specifically traveling to the United States, as well as the different visa types available.

### 2.1. US Visa Types

There are two broad visa categories available for individuals visiting or moving to the US, immigrant and non-immigrant visas. Immigrant visas are issued to foreign nationals who intend to live and work permanently in the US [34], while non-immigrant visas are usually for those seeking to enter the US on a temporary basis for example for tourism, business, medical treatment, education, or other forms of temporary work [33].

For the visa process, individuals are required to share a wide variety of documents, particularly highlighting ties to their home country and their intention to head back home after their trip in the case of non-immigrant visas. These documents and information are required from all visa applicants regardless of country of origin or application, and include filled visa-specific forms such as DS-160 and I-20 for students, demographic documents such as a valid passport, education and employment history, financial documents such as bank statements as well as medical records, birth certificates, etc. For example, those traveling from India to the US for education need to provide a valid passport, a

signed I-20 form from the school they will be attending in the US, proof of sufficient funds for tuition and other living expenses normally via bank statements or scholarships, and countries they have recently visited.

## 2.2. US General Visa Process

While the visa application process varies depending on the country the applicant is from or currently resides in, most US embassies require visa applicants to first fill out an online form where they can provide information relating to their travel for example the reason for the trip, places where the applicant will stay or visit, intended dates of the trip etc. Once this form has been filled out, applicants make a non-refundable payment for the visa before scheduling a visa interview. This payment typically ranges from \$160 to \$265 depending on the type of visa being sought or the citizenship or country of residence of the applicant [35].

For the interview itself, applicants usually speak to a consular officer at the embassy and provide any other supporting documents. Fingerprints and other bio-metric information are also collected as part of this process. The decision to grant or deny the applicant the visa is made by the consular officer. If the application is approved, the applicant leaves their passport at the embassy and can collect it after a few days with the visa stamped on it, or have the passport mailed back to them. Following, applicants can now travel to the US subject to their visa and other documents getting approved at the initial port of entry in the US. It is important to note that having a valid visa doesn't always guarantee that the applicant will be allowed entry to the US.

## 3. Related Work

**Challenges When Moving.** Several studies have investigated the challenges that people face when moving to a new country, and the measures they undertake to navigate these challenges. Through a three-month study exploring the challenges that Iranian immigrants in Canada face when transferring money to and from their home country, Rohanifar et al. [46] found that many Iranian immigrants rely on informal financial services for better real-time exchange rates, less bureaucracy, and overall better flexibility. They highlight that financial activities and behavior are often shaped by contemporary global politics and the cultural values of the community.

Through a series of workshops with 70 adult “newcomers” enrolled in colleges in Sweden, Coles-Kemp et al. [10] found that while mobile phones offer security and a safe space for individuals to establish a new life after moving, their usage, unfortunately, produces some threats and vulnerabilities beyond those traditionally envisioned regarding the use of mobile phones. Through another study with 132 “newcomers” to Sweden, Coles-Kemp et al. [9] noted that when communities are dealing with high levels of precarity, they are more likely to prioritize accessing the benefits of a service rather than being concerned about its security.

By exploring the perspectives of people that gather, maintain, and utilize data generated as people move to

Canada, Shankar [49] found that a range of stakeholders work together in the collection and use of this data, including settlement service providers, migrant justice activists, immigration researchers, government staff, and designers of digital systems for newcomers. The study proposes a framework for keeping the data of newcomers safe.

To help immigrants easily move and settle into their new countries, smart card technology has been proposed due to its ability to create strong identity credentials that can protect peoples' identities as well as enable their immigration status and employment eligibility to be easily verified [2]. More recently, social media, particularly Twitter, has proven to be a good source of information for those moving as well as for researchers exploring concerns of migrants and refugees [21]. For instance, Syrian immigrants moving to the Netherlands rely on social media information from their social ties, especially information based on personal experiences [12]. Walsh et al. [53] have recently explored Twitter usage by federal agencies tasked with border security and migration policing in Australia, Canada, and the US, finding that it is mainly used for broadcasting information, managing impressions, and enlisting public assistance.

Challenges when settling into new countries have also been explored, with Simko et al. [50] showing that recently resettled refugees in the US face significant security and account management issues, and consequently rely on their case managers for assistance navigating them. Similarly, Slupska et al. [51] explored privacy and security threats of migrant domestic workers in the UK and found government surveillance, scams and harassment, and employer monitoring to be primary threats. By examining refugee resettlement in Sweden from a Human-Computer Interaction (HCI) perspective, Jensen et al. [19] noted that the resettlement digitization employed in Sweden amplifies barriers to resettlement of refugees despite helping expedite the resettlement process.

Building on these studies, our work explores the experiences of those moving to the US **throughout** the moving process. We unpack, for instance, the role of “cultural orientation” and other elements of the immigration process as experiences that shape immigrants' security and privacy experiences as well as their threat models.

**Risks When Sending Sensitive Documents.** Warford et al. [55] have recently investigated the strategies and perceived risks of sending sensitive documents, finding that most participants are likely to recognize the risks at the destination. Despite security risks, Warford et al. further found that most participants are satisfied with existing methods of sending documents. While Warford et al. focus on sensitive documents with participants from the US, our study explores challenges and concerns for those moving from other countries to the US, including the documents they have to share, as well as security and privacy risks, concerns, and behavior throughout the moving process.

**Security and Privacy Advice.** Previous studies have examined where users get security and privacy advice from, and what motivates them to follow or not follow recommended

advice. Through semi-structured interviews followed by an online survey with participants from the US in 2015, Ion et al. [18] found differences between what experts and non-experts consider important advice for staying safe online, with experts considering updating their apps and operating system, selecting unique passwords as well as using password managers as important. Non-experts, on the other hand, mentioned using an anti-virus, using strong passwords as well as frequently updating them as paramount. Busse et al. [7] recently confirmed these findings with European participants.

By asking participants to provide search queries for security advice followed by a comprehensive collection and analysis of advice on the web, Redmiles et al. [44] noted that users find most security imperatives actionable and comprehensive, but struggle to prioritize; similarly reported by Reeder et al. [45]. Some studies have also shown that advice sources are influenced by socio-economic classes [42] while others [14] have shown the security vs convenience tradeoff users have to make when following recommended advice, with users that are likely to follow advice, rating its benefits higher than its costs. Other studies have shown that security advice with a lot of marketing information is less likely to be followed by users [43]. Our study investigates sources of advice for people moving to the US and its impact on their digital security and privacy in the moving process.

**Demographics' Impact on Security and Privacy.** Demographics and access to digital services (or lack thereof), influence peoples' security and privacy behaviors. Through a qualitative study with 40 low-literate, low-income participants from Pakistan, Naveed et al. [31] found gendered differences and highlighted the impact of patriarchal norms and religious beliefs on men's and women's understanding and management of privacy. Women are often excluded from public spaces, giving them fewer opportunities to learn about digital devices and privacy or security advice. Moreover, women's association with privacy and their desire for privacy is seen as scandalous and inappropriate, discouraging them from adoption. This study highlights how different cultural associations that are often in place when moving abroad can impede the adoption of good security and privacy practices.

In a study with 563 participants from the Caribbean region, Wilkinson et al. [56] found that being a previous victim of threats increased participants' perceived vulnerability and severity of harm, leading to elevated safety protection behaviors. By focusing on Turkish immigrants to Germany, Bozdağ [5] found that education, social status, and cultural background affect how Turkish migrants connect digitally back home with their families. Liaquat [23] has recently suggested the use of technology incorporating story-telling approaches with marginalized communities to help them learn languages, preserve family histories, and share cultures.

Our study explores the challenges and concerns, especially related to security and privacy, that people face when moving from different countries to the US. We additionally find that participants' sources of advice seem to be influenced by the specific visa being sought, with those moving for

employment getting advice from their employers while students primarily rely on their friends and family.

**Understudied Populations.** Recently, a growing body of research has investigated security and privacy challenges in understudied or marginalized populations, highlighting the need for more consideration of these groups in security and privacy design. Through investigations of the usage of technology among refugees in the United States [50], mobile loan apps [28] and cybercafes [29] in Kenya, previous studies have shown that security and privacy are not always a priority for disadvantaged groups due to other competing needs. Women in South Asia employ various techniques including content deletion to protect their privacy due to an expectation to share their phones with others in the household [48], while sex workers view broad security and privacy tools as insufficient and are therefore forced to take additional measures to protect themselves online [25], [3].

Some researchers have focused on understudied populations that are additionally at-risk, including undocumented immigrants [17], precarious migrants [32], incarcerated people [36], [37], Muslim-American women [1], protesters [4], human trafficking survivors [8], journalists [27], activists [11], and older adults [41], [15], [40], unearthing unique security and privacy challenges that require more nuanced solutions. By identifying the risk factors that amplify digital safety threats to these groups, Warford et al. [54] have recently developed a framework that can guide the study of these users as well as positively support technology design that accounts for their specific needs.

Our work complements and supports this growing line of research by exploring challenges and concerns for people moving to the US, a population that has received little attention in the context of security and privacy research. We also show how power imbalances often supersede security and privacy concerns for such populations.

## 4. Methods

Our goal was to investigate the challenges relating to security and privacy that people face when moving to the US. In this section, we describe the interview procedure, recruitment, data collection and analysis, limitations, as well as ethical considerations of our study. Lastly, we discuss how our subjectivity and other experiences as researchers likely influenced the study design and its outcomes.

### 4.1. Instrument Development

The interview guide was developed around our research questions. To identify gaps, we first examined previous work on the challenges that people commonly face when moving to a new country. Combining this with our own experiences moving to the US, we devised questions to investigate the type and scope of information that people are required to share before, during, and after the moving process, as well as any concerns with this throughout the process. We also inquired about the challenges people face during this process,

particularly relating to security and privacy followed by any adverse experiences such as scams or fraud encountered. Lastly, we asked participants about their sources of advice during the process. The full interview guide is available in Section A of the Appendix.

Most of the researchers in the team have recently moved to the US from another country. Therefore, we tested the interview protocol with some of these researchers acting as participants, and used the feedback from these interviews to iterate the interview guide and to improve both the clarity as well as the flow of the questions.

## 4.2. Recruitment and Demographics

We recruited 25 participants from 17 different countries holding 13 different visa types for semi-structured interviews between July and October 2022. We first recruited through personal contacts. This allowed us to directly contact suitable interview participants who matched all our requirements. Afterward, we recruited through social media platforms by posting a recruitment flyer on a Twitter account with a large international following, as well as stories on Instagram. We also posted a message in a WhatsApp group for international students in the Washington DC area. These channels are commonly used by our target group and allowed us to reach a wider range of potential participants. After exhausting these strategies, we switched our recruitment to Prolific, an online recruitment platform that further allowed us to reach a broader and more diverse sample.

To be eligible for the study, participants had to be at least 18 years old and English-speaking. Participants were also required to have legally moved to the US for the first time in 2017 or later. We chose these recruitment requirements to minimize language barriers, outdated information, or any legal risks to participants. Most participants were young women that had moved to the US aged between 17–29 (13), and had moved for work (13) or school (5). Table 1 provides a more detailed view of the demographics of the participants.

## 4.3. Interview Procedure

We used Calendly to schedule all interviews. Prior to the interviews, participants received and consented to the study consent form. Interviews were then conducted on Zoom by one researcher who acted as the lead interviewer, with another researcher often present to take notes. All interviews were conducted in English and lasted 43 minutes on average, with the shortest and longest interviews lasting 26 and 79 minutes respectively. The interviews were all audio-recorded and later transcribed using a GDPR-compliant transcription service. Each participant was compensated with a \$20 Amazon gift voucher or Prolific credit for participating in the study.

## 4.4. Data Analysis

We used open coding to qualitatively analyze the data [47]. Two researchers first met to discuss the overall

structure of the codebook and the codes to use. Afterward, they each independently coded four interview transcripts to create an initial codebook. As part of this process, they regularly met to collaboratively resolve disagreements, update, and further refine the codebook. Following best practices, [24], one researcher was assigned the role of a primary coder and coded all the remaining transcripts. The primary coder was also responsible for maintaining, updating, and iterating the codebook. The other transcripts were coded by five secondary coders. The secondary coders met with the primary coder regularly to resolve disagreements and update the codebook. This approach does not require the calculation of inter-coder agreement, with conflicts resolved as they emerge. The entire team then met to discuss broader themes emerging from the interviews following McDonald et al.'s [26] best practices for qualitative research.

## 4.5. Limitations

Our study has several limitations. First, as this is a volunteer study limited to only participants that have recently moved to the United States, only participants that wished to take part did. Therefore, we may have failed to capture important information from participants that chose not to participate. Similarly, restricting the study to participants that moved to the US legally means we potentially missed out on crucial information from undocumented immigrants. However, we purposefully did this to avoid any potential harm to these participants; future work can explore the challenges faced by undocumented immigrants as well as people moving to other countries or places.

Another potential limitation of our study is language barrier. While all participants were required to be English-speaking, the translation of specific documents or information from their country of origin might be inaccurate despite our best efforts. As is also typical with interviews, our sample size was relatively small, and skewed towards younger participants. However, we made all efforts to recruit diversely from different countries and only ended data collection after reaching saturation. We further restricted eligibility to participants that had only moved to the US in 2017 or later to ensure participants could recall the process and the challenges and concerns they faced.

Some aspects of our results, including visa appointment wait times and interview procedures might have been impacted by the COVID-19 pandemic. Notably, as the virus spread, the US issued travel bans and initially closed its borders to people from China followed by countries that reported high infection rates [16]. In some cases, US consulates abroad were closed off all together, contributing in part to abnormally high visa appointment wait times [52]. For the consulates that remained open, some measures including social distancing, mask mandates and later on vaccine requirements were enforced [16]. At the same time, however, the interview procedures did not change much from pre-pandemic processes, with interviews traditionally held in public spaces in the vicinity of other visa applicants; thus, while interview data was collected after the start of

TABLE 1: Participants' Demographics

ID	General information			Visa & move related information			
	Age at Move <sup>1</sup>	Gender	Occupation	Visa Type <sup>2</sup>	Country of Origin <sup>3</sup>	Year Moved	Reason
P01	28	Woman	Student	Student F/M	China	2021	School
P02	20	Woman	Student	Student F/M	Brazil	2019	School
P03	17	Non-Binary	Student	Student F/M & G4	China	2018	School
P04	21	Woman	Student	Tourism/Vacation (B2)	Venezuela	2021	Tourism
P05	25	Woman	Employed	H1-B	Brazil	2018	Work
P06	25	Man	Employed	Student F/M	India	2018	Work
P07	26	Woman	Can't work	Dependent (H4)	India	2021	Dependent
P08	30	Woman	Employed	Returning Resident (SB)	Nigeria	2017	Work
P09	23	Woman	Student	Student F/M	India	2022	School
P10	34	Man	Employed	Exchange Visitor (J)	Rwanda	2021	Work
P11	35	Woman	Employed	Exchange Visitor (J)	Austria	2018	Work
P12	22	Woman	Employed	Exchange Visitor (J)	Kenya	2018	Work
P13	28	Man	Employed	(Dependent) Exchange Visitor (J)	Australia	2022	Dependent
P14	30	Woman	Homemaker	(Dependent) Exchange Visitor (J)	Sweden	2020	Dependent
P15	26	Man	Employed	Student F/M	India	2017	School
P16	34	Woman	Employed	Spouse of a US citizen (IR1, CR1)	Vietnam	2021	Work
P17	34	Man	Employed	TN NAFTA	Canada	2022	Work
P18	36	Man	Employed	E1	Germany	2020	Work
P19	22	Woman	Employed	Fiancée of US citizen (K1)	United Kingdom	2019	Reunion
P20	32	Man	Employed	L1	India	2019	Work
P21	29	Woman	Employed	Fiancée of US citizen (K1)	Malaysia	2021	Marriage
P22	43	Man	Employed	L1	China	2019	Work
P23	30	Man	Self-employed	Green card	Phillipines	2022	US citizen
P24	30	Man	Employed	H1-B	Hong Kong	2018	Work
P25	29	Man	Employed	H1-B	Malaysia	2021	Work

<sup>1</sup> This was the age of the participants during the time of their move to the US. All participants were at least 18 years or older at the time of the interview.

<sup>2</sup> Some visa types were self-described by the participants. <sup>3</sup> The country of origin is not always the same one that participants applied for a visa from.

the pandemic, the privacy concerns with open spaces for interviews are in line with pre-pandemic practices.

Lastly, the data quality may have been affected by scammers as some participants signed up for the study despite not meeting the eligibility. This was particularly the case for some participants recruited from social media. However, we asked participants to fill out an eligibility form where they provided some personal details as well as some information about their move on signing up. Before starting each interview, we asked participants these questions again and ended four interviews where the participant responses were inconsistent. We additionally reviewed each interview afterward, discarding two suspicious responses.

#### 4.6. Ethical Considerations

This study was approved by our Institutional Review Board (IRB). We provided all participants with consent forms and informed them of the purpose, procedure, and risks associated with participating. We also asked for consent before audio-recording and offered appropriate solutions if participants were not comfortable being recorded, for example simply taking notes. Additionally, we allowed participants to withdraw from the study at any time or skip questions that they did not feel comfortable answering.

Information such as Prolific IDs, emails, and social media handles may have been captured as part of the recruitment and scheduling procedure. However, this information was not recorded as part of the interviews or associated with the participants in any way to protect their privacy. Additionally, we collected participants' gender, countries of origin,

and levels of education to provide context to our results. All other personally identifiable information was redacted when transcribing the interviews as well as reporting the results, with all recordings deleted afterward. The emails collected were only used to disburse gift vouchers and were immediately deleted afterward.

Lastly, our study only focused on participants that had legally moved to the United States; we excluded participants that were either undocumented or had moved illegally to minimize any harm that may be caused by the potential disclosure of their information.

#### 4.7. Positionality Statement

In this study, we regard our subjectivity as a resource that helped us conduct the research more reflectively, by informing our research questions and our lens on the data [22]. The research team consists of eight researchers, seven of whom moved to the US under various circumstances including moving with family during childhood, moving for education, and moving for job opportunities. Our varying experiences enabled us to focus on the nuances and intricacies of the moving process, which we might have otherwise overlooked. For instance, we shed light on various facets of the process such as document translation, challenges when creating new accounts in the US, payment issues that participants might have potentially faced, etc. We have a first-person understanding of the vulnerabilities, efforts, and frustrations experienced in moving to the United States, which both helped engage with participants and create the research

narrative. Further, our security and privacy background as researchers helped us to specifically talk to the participants about security and privacy concerns and challenges they experienced. Finally, our analysis of the data follows an open-coding method and a personal understanding of these situations that further helped inform our methodology.

## 5. Results

We now turn to our results about the security and privacy concerns, threats, advice, and associated barriers to security and privacy throughout the process of moving to the US. We organize our results around our research questions outlined in Section 1 by first discussing participants' concerns and fears with the process as well as actual experiences that came up in the interviews (Section 5.1 and 5.2). We then turn to the bureaucratic and technical barriers that contribute to the security and privacy unease and issues participants faced (Sections 5.3 and 5.4). Finally, we discuss the advice they received, specifically focusing on the availability and lack thereof security and privacy advice, and its overall impact on their digital security and privacy (Section 5.5). As our study is qualitative, we do not report counts to avoid implying generalizability, but instead, use words such as "few" or "most" to highlight the prevalence of common themes.

### 5.1. Perceived threats, risks, and concerns throughout the visa process

We begin by exploring participants' concerns and perceived threats and risks throughout the visa process, focusing on the discomfort and potential for security and privacy harms stemming from the amount and variety of sensitive information required in the visa process. All participants were required to share multiple documents with various entities both prior to and after the visa application process. A lot of participants' threats and concerns centered around feeling uncomfortable sharing sensitive documents of themselves but also documents containing personal information of others as well as how this information could be misused in case of leakage. In this section, we provide an overview of the most common documents and information participants had to share, their associated risks with sharing these documents and any concerns as well as their overall perceptions regarding sharing them.

**5.1.1. A wide variety of sensitive information and documents are required during the visa process.** As discussed in Section 2, applying for a US visa involves supplying a multitude of documents containing personal and familial history, and differs by countries. Participants mentioned providing demographic information, education records, financial information (e.g., bank letters, statements of assets, company sponsorship), medical records, as well as reasons and plans for their stay in the US (e.g., school acceptance letters, travel plans). Participants who applied for a dependent or a spouse visa were required to submit proof of their relationship to

the embassy via birth certificates for dependents or marriage certificates or wedding photos, or sometimes even private chat histories for spouses.

**5.1.2. Some participants trust official entities with their information.** Some participants stated that they trusted the official entities they interacted with since:

*"these are not just ordinary people that just teach you on. They are licensed people, they have the mandates, they have the authority to ask you to bring documents"* — P08 (Work, Nigeria)

However, one participant was uncomfortable sharing their address, citing they were worried about being tracked. They further expressed some mistrust towards the US government and explained how this could affect them:

*"They are maintaining my record and they can use it whenever they want to if they want to search my history. So that is a concern I have even today. USCIS<sup>1</sup> maintains my record and they know where I stay, what I do, and everything. So they can come to my house at any time and check my records. So that's a concern I have."* — P15 (Student, India)

Although all participants in our study complied with the visa process, they were not all comfortable with the process, as we explore in the remainder of this section. They mostly adhered to the process as they felt they had little choice.

**5.1.3. Concerns regarding sharing financial information.** While most participants understood why *their* financial information is required, some participants were concerned, particularly with sharing financial documents of their family.

*"If they had a question about me, I would definitely answer, but giving my parent's personal information, I felt what they were doing was [sic] little awkward."* — P15 (Student, India)

One participant was concerned about misuse and leakage of this information and how this could potentially put their family at risk for example by attracting robbers. For instance, one participant was concerned about releasing her parent's bank statements as this information could also be used to threaten and extort her:

*"The immigration asked for it and I had to release this record to them and from there, people will know how much money my parents have and that could put me in danger."* — P03 (Student, China)

**5.1.4. Providing proof of relationship for those seeking spouse visas made participants uncomfortable.** For those seeking spouse-related visas, some participants expressed discomfort in sharing personal documents like wedding photos to prove their relationships. One participant did not

1. U.S. Citizenship and Immigration Services (USCIS) is an agency of the US government in charge of naturalization and immigration.

understand why their wedding photos were required and felt that this not only violated their privacy but also goes against the cultural norms in their community:

*“I personally felt that’s unnecessary, that’s not required. To be honest, the interviewer asked for the photos as well. I just had to show a few of my wedding photos as well. It was a small pocket album that I carried with myself. That was one silly thing which I felt it’s not required. [...] I felt funny. Why should I show my photos? Is it really required?” — P07 (Spouse, India)*

Though none of the participants had experienced tangible harm due to the information shared during the visa process, their concerns highlight the implications of future data leaks or political changes and how data shared during the visa process may have political, legal, financial, and physical consequences for applicants and their families.

**5.1.5. Participants felt uncomfortable sharing required documents.** When asked about how they decided with whom to share documents and information, most participants felt like they had no choice but to share the documents and information they were asked for in order to receive their visa. Most participants stated that they did not really deliberate over sharing documents, due to their obligation to share whatever they were asked for:

*“I didn’t really think about it, I just gave them what they asked me for.” — P02 (Student, Brazil)*

Several participants described feeling powerless about sharing documents, mainly because they were not sure why certain documents were needed, but shared them anyway out of fear of being denied services:

*“This is a standard procedure [...] If I want to live here, I have to do it. That’s it. Like getting vaccinated, this is the procedure. If I don’t want to share, I can go.” — P10 (Work, Rwanda)*

Others stated that they would not share this information if they had a choice:

*“I felt they were poking into some of my personal things. [...] it’s poking into my personal space. If I had an option, I wouldn’t want to share it with them.” — P15 (Student, India)*

We also found that several working professionals and dependents indicated that they did not know which of their personal documents had been shared with the embassy because their employer or spouse filed the visa application on their behalf. Often, they had shared this information with their employer at some point but did not remember later:

*“I think the hospital might have handled that because I don’t remember submitting those. However, I submitted them to the hospital when I applied for the job. When I applied for the job process with the hospital, I had to submit all my medical records*

*to show I was vaccinated. Maybe that’s why I didn’t turn in anything to immigration because the hospital had all the documents.” — P25 (Work, Malaysia)*

These results highlight the complexity and power dynamics involved when choosing whom and how to share documents and other personal information with during the visa process, particularly for applicants whose visa applications are filed on their behalf e.g., dependents. Participants have no overview over their documents and do not know which entity possesses which of their personal information.

## 5.2. Exacerbated online threats and vulnerabilities

When moving to a new country, individuals are often required to follow many new processes that they may not be familiar with. This may make it harder for them to distinguish between legitimate information and fraud. In this section, we discuss some of the heightened levels of online threats that participants faced as well as how these threats can lead to privacy and security violations including increased susceptibility to scams.

**5.2.1. Participants were vulnerable to scams when renting from abroad.** One concern that came up frequently in our interviews was about housing scams. Students were required to rent a place in the US as well as sign a lease in advance of their travel. A vast majority of them were not able to view the apartment and the environment in person before moving and had to make a binding decision online. This made them particularly susceptible to rental scams. Most students seemed very concerned and cautious of housing scams and false online postings:

*“I had to rent a house before I came to the U.S., and I couldn’t see the house and I couldn’t see the rest of the environment before I rented it. [...] You just had to believe the other. If you are lucky, it’s real, if you are unlucky, you will lose your money yes.” — P01 (Student, China)*

Most student-participants looked for housing through their university housing website, rental websites, and Facebook communities. While some of these sources, e.g., university housing websites, may be more trustworthy and official, landlords and postings on these websites are not always vetted by the respective employer or school.

**5.2.2. Some participants were the target of phishing and scam calls after moving to the US.** Most participants mentioned scam emails, phone calls, and false online postings as a threat. One participant mentioned receiving a call from a fake Immigration and Customs Enforcement (ICE) agent who told them that some of their visa application documents were missing and that they would be deported if they failed to provide the information:



*“I did actually receive a scam call from someone pretending to be an ICE (Immigration and Customs Enforcement) agent [...] He said that, you know, I had some documents that I did not submit through and because of that, my application is going to be suspended or cancelled or something, and I’m at risk of deportation[...] Then I just told him that I know that you’re trying to trick me because I know that I have submitted all my documents and there’s nothing going on with my application at the time. Then he tried a scare tactic. He said, someone has a copy of my passport, and they are using it for identity theft, which is a totally different scam at that point.” — P21 (Spouse, Malaysia)*

Another participant, who was unfamiliar with scams in the US, mentioned that they received an impersonation call from someone claiming to be a Department of Motor Vehicle (DMV) agent, and took their driver’s license and other information:

*“I received a call saying that the DMV needs your driving license details and your personal information. The person spoke as if that person was from the DMV agent. I was not aware and I gave away my driver’s license info[sic] and then I realized that it was a scam call [...]” — P15 (Student, India)*

One participant received a phishing call after leaving their bank and exposed their personal information once again due to unfamiliarity with scam calls in the US. They mentioned closing their bank account all together after realizing they had been scammed:

*“[...] the scammer pretended to be Chase Bank, so I was silly enough to provide some personal information until I realized that they were not Chase Bank, so I hung up on them. [...] I accepted the call because I just left the bank to withdraw some money[...] But after I realized that they were scammers, I hang up on them and called my bank immediately and basically closed my account.” — P16 (Spouse, Vietnam)*

Despite many participants mentioning scams as a concern, most were able to identify that they were scams and a majority had not, to their knowledge, fallen victim to any. Nonetheless, our results suggest that it is important to inform and educate visa applicants about common scams in the US (and other countries they may be relocating to) and how to identify and protect themselves from them.

### 5.3. Bureaucratic barriers to security and privacy throughout the moving process

Having explored the security and privacy threats and risks directly associated with moving to the US (Sections 5.1 and 5.2), we now explore bureaucratic and administrative

issues identified by participants that contributed to or directly caused these violations of security and privacy and feelings of unease, fear, or discomfort during the visa process.

**5.3.1. Unclear and missing information on embassy websites.** Most participants indicated that they struggled to get assistance from their respective embassy during the visa process. Most of the challenges participants faced were related to unclear instructions and information on the embassy’s website, insufficient support, shortages of visa interview appointments due to the COVID-19 pandemic, and a lack of transparency in regard to the visa processing status. These challenges can cause participants to turn to other potentially illegitimate entities for assistance, further putting their digital security and privacy at risk.

Two participants criticized government websites for using complex language, making it difficult for non-native English speakers to comprehend:

*“I was reading those really complicated and detailed [sic] with tons of substantive clauses and I was like, what the hell are these?” — P03 (Student, China).*

One participant complained about embassy websites seemingly not having sufficient information for less common visa types and did not find sufficient information on how to apply for their G-4 visa:

*“Even the consulate doesn’t have that, like I had to search on their website saying, how to get a G-4 from the consulate, and they don’t have information about the G-4 on their web page.” — P03 (Student, China)*

Unclear directions sometimes led to incorrectly completed forms, subsequently attracting unwanted fees. One participant misunderstood the instructions on the embassy’s website and applied to the wrong embassy, only realizing this after they had already paid the non-refundable visa application fee. Unclear instructions and resulting misunderstandings can also cause visa applicants to share their sensitive information with more entities than required, imposing additional risk on their security and privacy.

**5.3.2. Lack of assistance from the embassy.** When trying to address these challenges and concerns, participants mentioned receiving insufficient help from the embassies’ customer support:

*“Their help center was just not very helpful in a sense that it took a long time to respond, the time that we didn’t have. I think we left a couple of message [sic] to the customer service email. But we never heard anything from them.” — P16 (Spouse, Vietnam)*

P03 *“called them and they were not in session that day.”*

As we discuss further in Section 5.5, the lack of sufficient clarity and help from embassies can be at best frustrating and at worst harmful if visa applicants expend more energy

and resources than necessary throughout the already-arduous visa process, and dangerous if visa applicants are scammed by someone offering illegitimate assistance.

**5.3.3. Lack of physical privacy during consular visits.** The physical structure of US embassies and consulates, as well as how officials used those spaces, caused privacy violations and discomfort during visa interviews. This is because the visa interviews at most US embassies are administered in an open space that is shared with other waiting applicants. This unfortunately means that applicants can overhear other applicants' interviews. One participant was uncomfortable being interviewed right before all the other applicants at the embassy as other applicants were able to hear all their personal information and other travel plans:

*"It is weird to be interviewed about this kind of stuff with other people around [...] There were maybe 20, 30 other people in the room while you're being interviewed so people can hear you."* — P02 (Student, Brazil)

This lack of privacy is particularly concerning when combined with participants' concerns about potential harms to those in their home country if data were to leak as discussed in Section 5.1.3.

**5.3.4. Fear of losing important paper documents during the visa application process.** A common way of sharing documents and receiving passports from the embassy after visa approval is through postal services. About half of the participants reported receiving their passports with their visa stamps by mail, whereas the other half physically picked up their passports from the embassy. While some participants were not concerned about receiving their documents by mail, several participants reported feeling concerned about losing their passport in the mail since this is an important identity and immigration document. Two participants applied for their visas in a foreign country and were worried about losing their passports:

*"I had some concerns about that maybe getting lost in the mail or something like that. That's my only ID, it's my name, it's got the visa [...]"* — P14 (Spouse, Sweden).

P15 (Student, India) similarly added that, "[...] when I'm in a country that is not my country, then I don't like being without a passport." Another participant was skeptical about the safety of postal services due to past negative experiences involving their friends:

*"The USPS is not the most reliable thing, you can imagine. My friend's passport was almost lost by the postal service."* — P03, Student, China

A few participants misplaced or lost documents like passports (P06) or documents needed for visa processing (P04). This, in turn, caused delays in visa appointments. Some participants were even forced to return to their home countries to be reissued with new visas. These cases highlight

how bureaucratic processes or administrative rules add to applicants' feeling of powerlessness and unease and can also have an impact on their digital security and identity.

**5.3.5. Challenges relating to Social Security Numbers (SSNs).** After moving to the US, participants encountered several challenges with their SSNs. Most participants struggled with obtaining an SSN because of long delays or having to first get a job. This, unfortunately, meant that they could not apply for a credit card, loan, or driver's license which are essential for living in the US:

*"I needed a Social Security Number to get my card, but you need to get a job to get your Social Security Number, so I didn't have a credit card before I got my first job."* — P01 (Student, China)

Some participants had restricted access to bank features:

*"I had to wait for more than one and a half months to get an appointment with the Social Security office. That was a bit challenging because I worked without a Social Security Number for the first two months. Therefore, I didn't have full access to the bank."* — P10 (Work, Rwanda)

One participant was frustrated after waiting for a year for their SSN due to a mistake in the IT system of the SSN administration:

*"It took me one year to get the Social Security Number. I talked to, I don't know, 20 people in several departments and Social Security office. Nobody could give me an answer why I did not receive the number. It turned out they did not update their IT systems with my name and the correct address[...] I wasn't existing in their system. I was living in the US, but not for the Social Security Office. Nobody could tell me why I have a problem."* — P18 (Work, Germany)

Given the number of authentication and identification processes that use one's social security number (or part of it, e.g., the last four digits), not having a social security number can be extremely detrimental. For instance, individuals may be unable to authenticate, or change the security and privacy properties of their accounts. They may also be blocked from accessing certain services all together.

## **5.4. Technical security, privacy, access, and usability issues caused by new geographical restrictions**

In addition to procedural challenges that make participants vulnerable during the visa process, we further found that participants encounter technical challenges during and after their move to the US. These challenges often contribute to security and privacy issues, feelings of frustration, discomfort, and vulnerability as they have to use new technologies as well as provide more private information. Most of the issues mentioned by participants were specifically related to geographically-imposed restrictions on access to systems, software, or the telecommunications network.

#### 5.4.1. Restricted website access after moving countries.

After moving to the US, some participants had issues accessing certain websites from their home countries. P03 and P06 detailed how they were not able to access some websites once they were in the US:

*“Those [sic] access is blocked for some reason. I try to access the website, but it says the website’s not available. I don’t know if it’s the website down or it’s a country issue.” — P24 (Work, Hong Kong)*

To circumvent the geographical restrictions, some participants resorted to using Virtual Private Networks (VPNs). For example, one used a VPN to access an Indian government website to help their parents update some information:

*“I wasn’t able to access so I had to get connected to a VPN[...], there were a few Indian government websites where I had to access and update certain things for my parents, so I wasn’t able to access. All I had to do was connect to a VPN and then get connected [...].” — P07 (Spouse, India)*

While VPNs were originally developed as a privacy-preserving technology to facilitate private transfer of data and information across public networks, our work as well as previous studies [30], [20], [13] show that VPNs are increasingly being used to circumvent geo-filtering enforced by content providers. Even though some of this geo-filtering is necessary for example in the case of copyright or licensing agreements, it still unfortunately locks out legitimate users in some cases, particularly when users move to new locations. Content providers should therefore re-evaluate the need to enforce geo-filtering, especially if it negatively affects their legitimate users. Where geo-filtering is necessary, there is perhaps an opportunity to educate legitimate users on alternative ways to access content and their information when they are in different locations, potentially via a VPN provided or procured by the content provider itself.

**5.4.2. Challenges with multi-factor authentication.** Some participants encountered challenges with multi-factor authentication where security codes or One Time Passwords were sent to their old phone numbers despite the fact that these numbers were no longer in service or use. Unfortunately, changing the phone number associated with the account without access to the previous phone number was almost impossible in many cases. For example, some struggled to access and ultimately change the phone number of some of their accounts without their previous phone number:

*“There are lots of accounts that in China I can’t use because they ask for a Chinese phone number verification. I had to change into all new accounts and that was a hard process because in order to change your phone number, you have to receive a verification code from your old phone number, but United States, I can’t receive messages from China. I don’t have my old phone number at all.” — P03 (Student, China)*

Challenges with multi-factor authentication after moving highlight how well-intended security measures can unfortunately inhibit account access for legitimate users. We argue that providers should consider availing alternative authentication mechanisms as well as broadly think about the implications of their design decisions on their end-users.

**5.4.3. Challenges accessing and downloading apps from app stores.** After moving to the US, some participants struggled to install apps from the US on their phones as they still had app stores of their home countries. As a workaround, P18 reported using another phone to install certain apps from the US app store:

*“Obviously, German private phone doesn’t work because the general settings need to be switched if you have Apple or Android, then you have to change your national market setting to the United States. I don’t want to do it with my German phone. I want to keep my German settings and this is why I cannot enter certain US services. They are simply not in the store. I have to use another phone. Certain, apps in America are not available in the store in Germany. That’s a problem.” — P18 (Work, Germany)*

In the course of downloading new apps from app stores after moving, participants may inadvertently download malicious apps impersonating genuine apps. Further, challenges accessing app stores or downloading apps in their new location makes participants vulnerable to installing malware disguised as legitimate apps, particularly from third-party mirror sites. Future work can therefore analyze the extent of impersonating apps on official stores as well as the prevalence of malicious apps on third-party mirror sites with the goal of broadly protecting users.

**5.4.4. Payment challenges and concerns with credit cards.** Throughout the process of moving, participants experienced several payment challenges associated with credit card payment and international transactions. One participant particularly felt uncomfortable paying the visa application fee using their credit card because of past credit card incidents as well as a fear of credit card fraud:

*“I’m not comfortable because my card has been hacked before so I don’t know from where it was hacked. Because that’s the only way of payment, I have to stick to it. If I had have a different option, I would consider that.” — P15 (Student, India)*

After moving to the US, some participants struggled to make payments with their credit card or had issues with international transactions. This was due to their credit card not being accepted at certain places (P03) or being frozen due to unusual high bank activities in a foreign country (P03, P12). One participant mentioned that they were not able to make international transactions from the US and had to rely on VPNs (P06) while other participants complained about long transaction times and high bank charges for withdrawing and transferring money (P02, P06, P09).

To alleviate some of the concerns faced prior to moving, embassies should consider offering applicants alternative secure payment methods (e.g., paypal, virtual prepaid cards or mobile money) to ease security and privacy concerns. They should additionally consider providing more support to participants when they move or relocate to new countries.

## 5.5. Security and privacy advice

Our findings thus far show that the process of moving to the US — from applying for a visa to arriving and getting settled — can be a process that causes discomfort, confusion, and unease, particularly around sharing information and potential security and privacy violations. Given this lack of clarity, participants often sought and were given advice about navigating the moving process. In this section, we evaluate this advice as indicators of further issues and barriers to security, and advice sources, as potential solutions. This can help in identifying gaps and providing applicants with more reliable information sources throughout the moving process.

**5.5.1. Advice came from both official sources and participants' communities.** Most participants sought reliable information and recommendations regarding their move and visa interview. This was particularly from people who have similar experiences including family, friends, spouses, alumni, colleagues, or online communities (e.g., Facebook, Reddit):

*“There was a community of people who were in the same situation[...] I asked them for advice and yes, experience recommendations as such.” — P15 (Student, India)*

When seeking official advice regarding required documents and the visa process, participants visited the official US government websites or received help from their employer, school, or lawyer. Our interviews further revealed that students and working professionals generally received more assistance during their visa application process compared to dependents. While dependents generally rely on their partners, students and working professionals receive guidance from their schools and employers respectively.

**5.5.2. Generic and insufficient security and privacy advice.** A majority of participants sought general immigration and moving advice and did not particularly focus on security and privacy aspects. Almost all of them asked for advice regarding the visa interview and visa documentation. Most were also interested in general moving advice (e.g., housing, opening up utility accounts, personal safety etc.).

For security and privacy related advice, some participants received advice on how to handle and secure their social security number (SSN) from the social security office, university, and employer. They also received generic security and privacy advice from the same entities and their family on protecting important documents (e.g. passport, visa forms) as well as avoiding talking to unlicensed or unauthorized people. A few participants further mentioned receiving a

booklet with security and privacy advice from their bank, embassy, and lawyer regarding protecting themselves and being aware of security threats.

While most participants perceived the advice they received as helpful, three participants said the advice was *very generic* (P23, P24) and not *life-altering* (P02).

### 5.5.3. Lack of advice on secure data sharing practices.

In general, participants mentioned that there was a lack of security advice, especially around data-sharing practices. While most participants received and were aware of general security and privacy advice (e.g., don't share SSN, protect important documents, online cyber security behavior), specific concerns centered around not knowing whether to share personal information on third-party websites as well as a lack of knowledge on the legitimacy of those sites. One participant mentioned that they were *“skeptical about putting my social security number into Credit Karma”* (P02).

Overall, a majority of participants rely on advice from people with similar experiences when moving as these are oftentimes people they already know and trust (e.g., family, friends). While most participants received general advice regarding their SSN and common cyber security threats, most of them were not able to assess legitimacy of third-party websites and did not know whether to share certain sensitive information with them.

## 6. Lessons, Recommendations, and Conclusion

Through semi-structured interviews ( $n = 25$ ), we investigate the challenges and concerns, particularly related to security and privacy, that people face when moving to a new country, focusing on participants moving to the US. Overall, we find that sharing multiple sensitive documents and encountering several administrative, bureaucratic, and technical issues led US visa applicants to fear for their own and others' security, privacy, and safety, highlighting a direct connection between *bureaucracy, technology and digital privacy and security risks, concerns and perceptions* in the US visa process. Although the visa process is inherently and intentionally invasive, it must still *be* and *feel* secure, private, and safe to applicants. It is in the interest of the US to make the visa process as secure and private as possible—both in perception and practice—to safeguard its future residents.

In this section, we discuss broader themes from our study and propose recommendations for the US government, universities, and technology designers to support and protect the security and privacy of participants and their families when moving to the US. We specifically note that hardships related to moving to the US were reported across countries of origin and visa types, including countries with strong ties to the US. We, therefore, hypothesize that many hardships inherent in the visa process are not necessarily intentional, and it may be in the interest of the US to improve the process. Many of our recommendations may be generalizable to other groups with similar vulnerabilities.

**Administrative processes and bureaucratic policies amplify security and privacy concerns and issues during the visa process, rather than mollifying or preventing them.**

Our results reveal how various non-technical administrative decisions shape the threat models and security and privacy experiences of those moving to the US. Visa applicants often feel uncomfortable, fearful, and violated throughout the visa application process due to inherent power dynamics between applicants and US government officials, as well as a lack of clarity on the process from official sources. We believe that these factors *magnify* and *create* security and privacy issues, concerns, and potential harms, in ways that at times seem orthogonal to the visa process itself, but are also potentially discriminatory. We thus strongly recommend the following types of procedural changes to reduce applicants' security, privacy, and safety concerns and risks:

*Recommendation for the US government and local third parties:* We urge embassies and consulates to improve the clarity of the visa process by, for example, providing visa information in *less legalese language*, and providing *complete* information about document requirements, timelines, and the basis on which decisions are made. Embassies and consulates might consider, for example, workshops to aid potential or hopeful applicants, in order to demystify the process. Without a clear vision of the visa process and information required, applicants may feel unsure where their data will go—intentionally or unintentionally—and feel violated by officials' requests for certain information (Section 5.1).

Enabling applicants to understand the process and information required—including any alternative options for certain requirements—ensures they make an *informed* decision about entering and remaining in the visa process and is a critical part of respecting visa applicants' autonomy, time, and money. Because local or cultural norms around the sensitivity of certain personal information means that some applicants may feel violated or concerned with sharing certain information, it is also important that officials request information in a way that is consistent with and sensitive to local norms in order to reduce discomfort for applicants.

*Recommendation for the US government and technologists:* Ensure information transmission in a manner that both feels secure and private to applicants and is consistent with current security and privacy standards. For example, consulates and embassies should ensure applicants have sufficient physical privacy when speaking with officials, especially about sensitive or personal topics (Section 5.3). Some participants were concerned about documents getting lost in the mail; perhaps requirements for physical documents could be determined based on local trust in and reliability of national post services. We also strongly recommend that the visa process must respect participants' threat models—which are shaped by local political and social context—regarding digital document transmission. Some applicants may prefer to physically show documents on their phone but not have them transmitted or recorded, while others may prefer to transmit them via an industry-standard secure document-

sharing portal [55]. Because of the effect of political and social context on threat models and technology usage [11], the preferred methods of document transmission *may vary*, and it is important to enable document transmission that (a) feels secure and private to the applicant, (b) meets the US government's standards for security and privacy, and (c) meets industry standards for security and privacy.

**A combination of the interaction with multiple entities, limited assistance, and being in a new environment make individuals moving to the US vulnerable to scams.**

Our results indicate that those moving to the US feel—understandably—confused and vulnerable throughout the process of moving. This is due to the multitude of entities they have to interact with, changes in sensitive information they have to keep safe (e.g., social security numbers), new adversaries (e.g., scams phone calls), and new administrative bodies and processes they have to interact with throughout. For instance, throughout the process of moving and settling into the US, we found that participants had to interact with multiple entities and share various sensitive and personal information about themselves as well as their families, especially during the visa application process. At the same time, unclear instructions and limited support from embassies coupled with being unfamiliar with their new environment in the US after moving made participants very susceptible to scams and other adverse experiences. Further, participants often had to rent out apartments in the US before moving, making them vulnerable to scams. After moving to the US, some participants were targeted with scam calls and phishing messages, with one participant having to close their bank account and open a new one after inadvertently sharing their personal banking information with a scammer (Section 5.2).

*Recommendations for schools and employers:* In addition to the recommendations made to embassies to improve transparency of the visa process as well as offer less legalese and local languages where possible, we encourage schools and employers to offer support to those moving, especially with regards to finding accommodation. While some schools and employers already offer such support, having a more centralized database with links to recommended accommodation options might be extremely helpful to those moving. Further, they can connect students or employees with others who have gone through similar processes, or are similarly looking for accommodation to make the process less intimidating. Moreover, schools and employers can also inform and educate those moving about common scams in the US as well as how they can protect themselves and their personal information such as social security numbers, for example through seminars or workshops or booklets with such information. As mentioned in Section 5.5.1, people moving to the US utilize online communities for help with the moving process. We did not conduct a comprehensive analysis of these online platforms. However, given the role that these platforms play in supporting applicants, future work can examine their role and impact in the moving process.

*Recommendations for technologists:* Those who move to the US may be more vulnerable to scams and spam because of unfamiliarity with their new environment. Our results show how work seeking to mitigate scams and spam in the US [38], [39] can also help a vulnerable group—those who have newly moved to the US. We encourage researchers and industry technologists to work together to continue to build stronger heuristics to identify and combat spam and scams.

**Certain design and security measures, even though well-intended, negatively affect legitimate users who have moved.** To restrict account and content access to legitimate users as well as enforce licensing or copyright agreements, websites commonly enforce geo-filtering whereby certain content or access is limited to particular geographic locations. Further, because of convenience, many two-factor (2FA) implementations use phone numbers whereby users receive authentication codes on their phone numbers through SMS. Despite their security benefits, our results with participants that have recently moved to the US show how these measures can negatively impact legitimate users. For instance, after moving to the US, some participants struggled to access certain websites back home because of geo-filtering as well as inability to receive 2FA codes because these codes were sent to their previous phone numbers which were either out of service or they no longer had access to. This often resulted in legitimate users getting locked out of their accounts. Some participants also struggled to download apps in the US as their phone app stores were still tied back to their home countries. This makes them susceptible to installing impersonating or malicious apps from third-party stores.

*Recommendations for technologists:* While some participants navigated some of the challenges e.g., using VPNs to circumvent geo-filtering, our results broadly suggest the need for technology designers to re-evaluate the impact of their design and security decisions on their users who move internationally. For example, all SMS-based 2FA systems should provide alternative authentication mechanisms in case users lose or no longer have access to their phone numbers. Websites or content providers that enforce geo-filtering should devise mechanisms to allow access for their legitimate users when they are in new locations, potentially by procuring, availing, and educating their users about workarounds such as VPNs. App stores could prompt users to switch their app store locations when people move to new locations to reduce challenges with app downloads. Some platforms may also predict an upcoming international move—much as credit card companies no longer require manual notification of travel to not flag card holders’ activity as fraudulent when out of their home area—with some confidence, prompt users about potential issues with authentication or access, thus allowing users to be *informed* and take actions that match their threat models and usability needs.

## Acknowledgment

We would like to express our deepest appreciation to Anna Lena Rotthaler, Anastassija Kostan, Jonas Kulawik, Joseph Ogren, and Karim Alami for their interest and invaluable input and feedback throughout this research. We also thank all the anonymous reviewers and shepherd for their thoughtful comments and feedback. This material is based upon work supported in part by the United States National Science Foundation under Grant Numbers 1845300 and 2206865, as well as by gifts from Google and Meta.

## References

- [1] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women. In *Proc. SOUPS*, 2022.
- [2] Smart Card Alliance. Securing identity and enabling employment verification: How do immigration reform and citizen identification align?, 2010.
- [3] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. “Disadvantaged in the American-Dominated Internet”: Sex, Work, and Technology. In *Proc. CHI*, 2021.
- [4] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proc. CHI*, 2021.
- [5] Çiğdem Bozdağ. *The Digital Bridge Between Turkey and Germany: Transnational Use of Digital Media in the Turkish Diaspora*, pages 157–172. Springer Fachmedien Wiesbaden, 2014.
- [6] Abby Budiman. Key findings about U.S. immigrants. <https://www.pewresearch.org/fact-tank/2020/08/20/key-findings-about-u-s-immigrants/>, Sep 2020.
- [7] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proc. SOUPS*, 2019.
- [8] Christine Chen, Nicola Dell, and Franziska Roesner. Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. In *Proc. USENIX Security*, 2019.
- [9] Lizzie Coles-Kemp and Rikke Bjerg Jensen. Accessing a new land: Designing for a social conceptualisation of access. In *Proc. CHI*, 2019.
- [10] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proc. CHI*, 2018.
- [11] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *Proc. IEEE S&P*, 2021.
- [12] Rianne Dekker, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk. Smart refugees: How syrian asylum migrants use social media information in migration decision-making. *Social Media + Society*, 4(1):2056305118764439, 2018.
- [13] Agnieszka Dutkowska-Żuk, Austin Hounsel, Amy Morrill, Andre Xiong, Marshini Chetty, and Nick Feamster. How and Why People Use Virtual Private Networks. In *Proc. USENIX Security*, 2022.
- [14] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Proc. SOUPS*, 2016.
- [15] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proc. SOUPS*, 2019.

- [16] Julia Gelatt and Muzaffar Chishti. COVID-19's Effects on U.S. Immigration and Immigrant Communities, Two Years On. <https://www.migrationpolicy.org/research/covid19-effects-us-immigration>, Jun 2022.
- [17] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proc. CHI*, 2018.
- [18] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one can hack my Mind": Comparing expert and Non-Expert security practices. In *Proc. SOUPS*, 2015.
- [19] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. When the Civic Turn Turns Digital: Designing Safe and Secure Refugee Resettlement. In *Proc. CHI*, 2020.
- [20] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. An Empirical Analysis of the Commercial VPN Ecosystem. In *Proc. IMC*, 2018.
- [21] Aparup Khatua and Wolfgang Nejdl. Struggle to Settle down! Examining the Voices of Migrants and Refugees on Twitter Platform. In *Proc. CSCW*, 2021.
- [22] Calvin Liang. Reflexivity, positionality, and disclosure in hci. <https://medium.com/@caliang/reflexivity-positionality-and-disclosure-in-hci-3d95007e9916>, Sep 2021.
- [23] Amna Liaquat. Intersectional Approaches for Supporting Casual Language and Culture Learning in Immigrant Families. In *Proc. CSCW*, 2021.
- [24] Kathleen M MacQueen, Eleanor McLellan, Kelly Kay, and Bobby Milstein. Codebook development for team-based qualitative analysis. *Cam Journal*, 10(2):31–36, 1998.
- [25] Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *Proc. USENIX Security*, 2021.
- [26] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 2019.
- [27] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *Proc. USENIX*, 2015.
- [28] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *Proc. IEEE S&P*, 2022.
- [29] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *Proc. IEEE S&P*, 2023.
- [30] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. In *Proc. PETS*, 2020.
- [31] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. "ask this from the person who has private stuff": Privacy perceptions, behaviours and beliefs beyond w.e.i.r.d. In *Proc. CHI*, 2022.
- [32] Mihaela Nedelcu and Ibrahim Soysüren. Precarious migrants, migration regimes and digital technologies: the empowerment-control nexus. In *Journal of Ethnic and Migration Studies*. Taylor and Francis Online, 2022.
- [33] U.S. Department of State. Foreign Affairs Manual (Non-immigrant). <https://fam.state.gov/FAM/09FAM/09FAM040201.html>, Dec 2022.
- [34] U.S. Department of State. Foreign Affairs Manual (Immigrant). <https://fam.state.gov/FAM/09FAM/09FAM050201.html>, Jan 2023.
- [35] U.S. Department of State's Bureau of Consular Affairs. VISA Fees. <https://www.ustraveldocs.com/de/de-niv-visafeeinfo.asp>.
- [36] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives. In *Proc. USENIX Security*, 2022.
- [37] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proc. CHI*, 2021.
- [38] Sathvik Prasad, Elijah Bouma-Sims, Athishay Kiran Mylappan, and Bradley Reaves. Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis. In *Proc. USENIX Security*, 2020.
- [39] Sathvik Prasad, Trevor Dunlap, Alexander Ross, and Bradley Reaves. Diving into Robocall Content with SnorCall. In *Proc. USENIX Security*, 2023.
- [40] HIRAK Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Warn Them" or "Just Block Them"? Comparing Privacy Concerns of Older and Working Age Adults. In *Proc. PETS*, 2021.
- [41] HIRAK Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why Older Adults (Don't) Use Password Managers. In *Proc. USENIX Security*, 2021.
- [42] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proc. CCS*, 2016.
- [43] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Proc. IEEE S&P*, 2016.
- [44] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proc. USENIX Security*, 2020.
- [45] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy*, 15(5):55–64, 2017.
- [46] Yasaman Rohanifar, Priyank Chandra, M Ataur Rahman, and Syed Ish-tiaque Ahmed. Money whispers: Informality, international politics, and immigration in transnational finance. In *Proc. CHI*, 2021.
- [47] Kathryn Roulston. *Analysing interviews*. The SAGE handbook of qualitative data analysis, 2014.
- [48] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.
- [49] Saguna Shankar. Coordinating migration: Caring for communities & their data. In *Proc. CSCW*, 2021.
- [50] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *Proc. IEEE S&P*, 2018.
- [51] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *Proc. USENIX Security*, 2022.
- [52] Sakshi Venkatraman. Indians face up to 3-year wait times for U.S. tourist visas. <https://www.nbcnews.com/news/asian-america/indians-face-3-year-wait-us-tourist-visas-consulates-subcontinent-are-rcna62499>, Dec 2022.
- [53] James P. Walsh. Social media and border security: Twitter use by migration policing agencies. In *Policing and Society, An International Journal of Research and Policy*. Taylor and Francis Online, September 2019.

- [54] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *Proc. IEEE S&P*, 2022.
- [55] Noel Warford, Collins W. Munyendo, Ashna Mediratta, Adam J. Aviv, and Michelle L. Mazurek. Strategies and Perceived Risks of Sending Sensitive Documents. In *Proc. USENIX Security*, 2021.
- [56] Daricia Wilkinson and Bart Knijnenburg. Many islands, many problems: An empirical examination of online safety behaviors in the caribbean. In *Proc. CHI*, 2022.

## Appendix A. Interview Questions

### Information Sharing

- 1) What info/documents were you asked to share to be able to move?
  - a) ...before moving to the US?
  - b) ...after moving to the US?
  - c) To whom did you have to share those documents?
  - d) How did you have to share the documents?
    - i) Was any of this secure or insecure? E.g., a public account, unencrypted SNS, or not secure postal service?
- 2) Did any documents require to be translated/notarized/proved to be authentic?
  - a) If so, what documents?
- 3) How did you decide with whom(person/entity) to share your private information?
  - a) Did you feel unsafe or uncomfortable sharing any documents or information throughout the whole process?
  - b) With whom?
  - c) Why?
- 4) Could you elaborate on how you sent these documents? Probe: e.g via a public account, unencrypted SNS, or not secure postal service?
- 5) How concerned were you about how protected your private information or documents were?

### Administrative and S&P Challenges

*If their visa application didn't go through on the first attempt:*

- 6) Can you tell us about what went wrong with your first attempt at obtaining a visa?
  - a) and what was different when your visa finally got approved?

*From here on, this is about BOTH the unsuccessful and successful visa process.*
- 7) Did you have difficulties with any documents that you needed to obtain?
  - a) Which documents and why?
- 8) Can you describe any difficulties you may have had with the U.S. admitting your documentation? (*prompt if they don't respond: E.g, you submitted something and it needed to be translated or had translation errors, or needed to be re-evaluated, or was misplaced, or had related other clerical errors.*)
  - a) Which document(s) and why was it difficult?
- 9) Were you penalized for anything that wasn't your fault? (Customs, lateness, non-response, etc.)
- 10) Which part of the moving process was the most challenging for you?
  - a) Why or why not? Can you elaborate?
- 11) Are you aware of any situation where your private information was unintentionally shared during or after the moving process? (Probe if needed: e.g., addresses, emails, birth dates, phone numbers...)
- 12) Are there any other challenges, with the move or visa process, not mentioned that you would like to tell us about?

### Scams and Adverse Experiences

- 13) At any time during the moving process from preparing the first visa application to after you moved: Was any of your information/documents/online accounts stolen/lost/forgotten? Examples: passport, credit cards, SSN, account login.

- a) If so, what did you do about it?
  - i) Report it? If yes, to whom?
  - ii) Why or why not?
- 14) Could you tell us if anyone else (not in an official position) asked for your private information?
- 15) How was your overall experience with the moving process? Would you recommend anyone to go the same route you did agency or church or private?
- 16) Did any services require you to pay?
  - a) What was the method of payment?
    - i) Did you encounter any problems with it?
    - ii) How could you tell if it was secure or not?
  - b) How much would you estimate that you spent on services for the process? (translating, notaries, shipping, other fees, etc.)
- 17) Did you encounter any scams or frauds that you were aware of?
  - a) If so, can you tell us more about that case?
  - b) How did you spot or identify the scam?
- 18) How do you protect yourself against scams or frauds?

### Sources of advice

- 19) Did you receive advice or help from anyone about the moving process? What kind of advice?
- 20) Or search for any advice?
  - a) If so, from whom?
    - i) Social media:
      - A) What platform or user?
    - ii) Agency:
      - A) What kind of agency? moving, immigration, legal, etc.?
      - B) Did you have to pay for their services?
    - iii) University:
      - A) Informal student organization? Official international student office?
    - iv) Employer
    - v) Friends or Family
    - vi) Any other sources that you can think of?
  - b) What advice did you receive in terms of S&P?
    - i) Would you say the advice is helpful?
    - ii) Did you encounter any conflicting advice?

### Technical Challenges After Moving

- 21) What new online accounts did you have to create after you moved? e.g Any online bank, school or work email, social media, etc. (*ask to elaborate if needed*)
  - a) Which information did you have to provide?
    - i) Anything that required proof of residency or an address, social security number, or any other information?
    - ii) Was there any information that you didn't (yet) have or did you encounter any other issues?
    - iii) Were there any circular dependencies with accounts needing each other to be created? E.g., *need a phone number for bank account, need bank account for phone contract*
- 22) How was your experience keeping yourself safe online after moving?
  - a) What method of authentication did you use? (*Probe: e.g., phone number/email/security Qs/location/authenticator app*)
    - i) What was your experience with authentication methods that you used?
    - ii) Did any two-factor authentications think you were not yourself but a malicious user instead?
      - A) If so, how long were you locked out/blocked?
      - B) E.g. new phone number so you can't access a security code with the old one, or location services not being in your country of origin
    - iii) How did you save passwords for these new accounts?
    - iv) What additional information did you need that you may have only gotten after your move? E.g. address, credit card, phone number, etc?
      - A) *If yes:* How did you access that information?



- Did you struggle to access that information?
- v) Are there any accounts in the country that you moved from that could not be accessed anymore?
  - A) What were the problems with access?
  - B) Did you get access again? How? E.g., *Did you have to share account information with anyone in your country of origin to get back into the account?*
  - C) Did you have to ask a friend/relative to access your account? E.g.: *By sharing passwords so they could verify that someone from the US is not trying to get into your account?*
- vi) Did you need a relative/friends' information/account to be able to obtain your own?
  - A) Can you explain what info and for what accounts?
- b) What are some other general issues that you faced after you reached the destination dealing with payments? E.g., getting a new SIM card, bank account, issues with credit cards?
  - i) Did you have issues getting a credit card? (or getting accustomed to local payment methods that are not primarily being used in your country of origin e.g. Google pay)
    - A) Anything that required proof of residency or an address?
    - B) Did you have any issues with having a credit score with purchasing/renting?
      - Examples: appliances like phones, laptops, cars, or renting an apartment, and loans
- 23) Is there anything else about security and privacy related to your move that we should have asked about?

## Appendix B.

### Qualitative Codes

- **Documents shared before move:** passport (20), work-related documents (11), personal/biographical information(9), transcripts/certificates from previous education(7), Proof of relationship (8), medical records (7), COVID-19 tests/vaccines (7), information about partner (6), birth certificate (5), financial statements (5), biometrics (4), information about parents (4), ID of country of origin (3), information about children (2), police clearance (1), SSN (1)
- **Documents shared after move:** visa & passport (14), US address (6), Arrival Report I-94 (6), financial statements (4), visa-related forms (4), driver's license (3), reason for move (3), information about parents (2), work authorization (2), COVID-19 tests/ vaccine (2), proof of relationship (1), medical records (1), school documents (1)
- **Mode of sharing:** in-person (23), upload digitally (12), share by email/digitally (9), mail documents (8), passport mailed to applicant (6), passport picked up at embassy (5)
- **Decision making:** gave what they asked for (10), did not really think about it (7), entity seems trustworthy (6), received detailed instructions from office/school/employer (3), own gut feeling (1)
- **Translation/Notarization:** No (15), yes (14), no issues (7), faced issues (2)
- **Shared with:** person at embassy (20), employer (11), customs/immigration (11), online visa portal (7), school (6), landlord/hotel rental(5), lawyer (5), bank (4), family/friends/spouse (1), social security administration (1), travel agency (1)
- **Feelings about sharing documents:** trust entity to keep it secure (15), had no choice (11), think it's standard procedure (11), doesn't care about documents (8), uncomfortable because information can be leaked (7), understand why documents are needed (7), postal service is secure (7), comfortable because people have mandate (6), uncomfortable sharing certain documents/don't know why need it (5), comfortable because in person (6), unsafe to send things out in mail (4), don't know if mailing secure (3), don't know if sharing digitally

- is secure (3), think their not potentially targeted (2), security depends on entity (2), don't trust entities (1)*
- **Frauds/scams:** not aware (13), phishing calls/text/emails (8), housing scam (1), phone number used by someone else (1), Facebook leak (1)
- **Payment method:** debit/credit card/bank (17), cash (6), online payment platform (4), check/money order (2)
- **Payment challenges:** high bank charges (3), POS system error (2), only credit card as payment method (feels uncomfortable using it) (2), has no credit card (2), money transaction took a long time (1), credit card not accepted (1), direct deposit error (1), credit card PIN issues (1), can't pay with home countries bank account (1)
- **Challenges:** getting a credit card/score (10), shortage of visa/SSN interview appointments (7), providing proof of residence (6), trouble getting some documents (6), getting all documents right (5), renting from abroad (3), transporting everything to the US (3), interview at different city/ country (3), forget important details (2), instructions unclear (2), adapting to new culture (2), get work authorization (2), need SSN for some living expenses (2), no time to organize move (2), currencies confusing (2), can't access post in country of origin (2), applying for a visa with insufficient language skills (1)
- **Concerns:** stressed about getting visa denied (6), documents being stolen/lost (4), being alone/leaving family and friends behind (4), offering sensitive information online (3), enter SSN online (2), visa interview not private (1), personal safety/ discrimination (1), being denied at immigration (1), not getting visa renewed (1)
- **Adverse experiences:** delay for some documents (6), no transparency on visa processing (4), mistakes on forms/systems(4), long time for visa approval (3), no help from customer service (2), long waiting times for visa interview (2), mail sent to old address (2), third party access to data (1), embassy website lack information for certain visa types (1), social security number shared over phone (1), shortened visa validity (COVID-19 related) (1), responsible person at embassy not present (1), misplaced passport (1), high fees because of third party usage (1)
- **Advice help/source:** Family/ friends/ spouse and people with similar experiences (19), Social media/internet (16), employer (10), university/school (7), lawyer (6), official government website (4), social security office (3), embassy (2), bank (2), self (1), security guard (1)
- **Advice content:** visa interview and immigration (18), visa documents (12), housing (8), SSN related (8), personal safety (7), emotional support (6), cyber security behavior (6), none (security & privacy related) (4), keep documents secure (4), moving advice (4), banking (4), work related (4), academic (2), obtaining driver's license (2), health insurance (1), recreation (1), setup US phone number (1), file taxes (1)
- **Advice helpfulness:** helpful (18), unhelpful (4), helpful but no great (3), don't know if helpful (1)
- **Missing Advice:** credit cards/ score (2), handling taxes (1), who to share data with (1), changes due to COVID-19 (2), certain visa types (1), prohibited items at immigration (1)
- **Accounts created:** bank account/ credit card (22), driver's license (9), SSN (8), utilities (7), visa/government accounts (5), work related (4), school accounts (4), private email (4), memberships (4), apps (3), social media(1), apple ID (1)
- **Challenges with accounts:** issues using old country phone numbers for MFA (7), remember passwords (6), foreign IPs blocked (4), no SSN without a job (3), can't transfer authentication to new phone (2), can't install US apps on international phone (2), 2FA recovery (2), forgot security questions (2), no US phone number yet (2), in-person to access accounts (2), restricted bank features (1), need old phone number to change phone number of accounts to new one (1), no driver's license without SSN (1), need friend's address (1), access accounts when back in country of origin (1), reach customer service (different time zone) (1), ID from country of origin not accepted (1), no two IDs (1)
- **Passwords:** Password manager (12), memory (7), Re-use passwords (5), write them down (4)

## **Appendix C. Meta-Review**

### **C.1. Summary**

This paper presents a security and privacy-centric look at the experiences of people moving to the US for the first time. The authors conduct semi-structured interviews of  $n = 25$  participants to understand the factors that go into moving to the US and how those factors influence susceptibility to security and privacy risks. The authors find that participants have a heightened risk of susceptibility to spam, scams, and fraud due to the visa granting process. The authors conclude with recommendations for regulators, employers, and technologists for improving the experiences of those moving to the US for the first time.

### **C.2. Scientific Contributions**

- 1) Independent confirmation of important results with limited prior research.
- 2) Addresses a long-known issue.
- 3) Identifies an impactful vulnerability.

### **C.3. Reasons for Acceptance**

- 1) The paper studies an important topic and provides a useful qualitative perspective on an issue that is

anecdotally well known.

- 2) The paper is well structured and well written, and is conducted with good scientific rigor for qualitative work.

### **C.4. Noteworthy Concerns**

The implications and recommendations provided in the discussion are too generic and not always directly actionable by the identified stakeholders. A deeper discussion of the tensions between participants' valid perceptions and concerns and the implicit goals of immigrant processes (e.g., deterrence, national security) should be included.

## **Appendix D. Response to the Meta-Review**

The reviewers note that some of our recommendations are generic and that we should add a deeper discussion of the tensions between participants' valid perceptions and concerns and the implicit goals of immigration processes. While very interesting, this was unfortunately outside the scope of our study, and did not come up during the interviews. Further, we argue that generalizable (rather than generic) recommendations are valuable because they may benefit populations other than the one we specifically explored.