Security and Privacy Experiences of First- and Second-Generation Pakistani Immigrants to the US: Perceptions, Practices, Challenges, and Parent-Child Dynamics

Warda Usman*[1] John Sadik*[2] Taha[3]
Ran Elgedawy[2] Scott Ruoti[2] Daniel Zappala[1]

[1]*Brigham Young University* [2]*The University of Tennessee, Knoxville* [3]*Purdue University*

***Abstract*—This work explores the security and privacy perceptions, practices, and challenges Pakistani immigrants face in the US. We also explore how parent-child dynamics affect immigrants' learning about and adaptation to security and privacy practices in the US. Through 25 semi-structured interviews with Pakistani immigrants, we find that first-generation immigrants perceive heightened risks of discrimination, surveillance, and isolation due to their status as Muslim immigrants. They also report tensions regarding self-expression and self-censorship in online settings. In contrast, second-generation immigrants quickly adapt to life in the US and do not perceive most of these challenges. We find that first- and second-generation immigrants mutually support each other in learning to use technology and reacting to perceived threats. Our findings underscore an urgent need for tailored digital safety initiatives and designs that consider the unique needs of at-risk populations to ensure their security and privacy. Recognizing and addressing these challenges can foster more inclusive digital landscapes, empowering immigrant populations with resilience and agency.**

1. Introduction

Globally, we are witnessing unprecedented levels of international migration. In the US alone, there are 44 million immigrants, accounting for 13.7% of the US population [1], [2]. Despite their significant presence, immigrants often find themselves marginalized, facing discrimination and prejudice in their lives [3], [4], [5].

Research into immigrant populations' security and privacy perceptions, practices, and needs is limited. Within the context of US immigration, we are only aware of three studies—one examining undocumented immigrants [6], one investigating refugees [7], and one studying the process of migration [8]. This paper contributes to this nascent body of work by exploring the experiences of legal, non-refugee immigrants from Pakistan.

According to the 2019 estimate by the Pew Research Center, Pakistani immigrants constituted the second-largest South Asian immigrant population in the US [9]. Pakistani immigrants navigate a complex set of challenges, including heightened scrutiny and stigmatization due to the intersecting factors of religion, culture, and immigration status, rendering them vulnerable to targeted attacks and stereotypes. We hypothesize that due to these factors, Pakistani immigrants in the US have distinct security and privacy needs that may differ from those of the general US population, though these needs may share similarities with those of other immigrant groups.

Recognizing the potential for inter-generational dynamics regarding technology use and learning among families [10], we also explore the interplay between first- and second-generation Pakistani immigrants. We define *first-generation immigrants* as those born and raised in Pakistan before migrating to the US, and *second-generation immigrants* as those born in the US to first-generation immigrant parents. Individuals who immigrated with their parents at a young age are sometimes called *1.5-generation immigrants*; for simplicity, in this work, we treat them as second-generation immigrants as, based on our results, they most resemble that group.

Our goal was to investigate the experiences of first- and second-generation immigrants, with a particular focus on the parent-child dynamics that shape these experiences. To this end, we conducted semi-structured interviews with 25 Pakistani immigrants, which included 15 first-generation immigrants and 10 second-generation immigrants. First-generation immigrants were parents, while second-generation immigrants were individuals with living, first-generation parents residing in the US. The interview questions were designed to capture distinct perspectives: first-generation participants reflected on their roles as parents, whereas second-generation participants focused on their experiences as the children of immigrants. Through these interviews, we sought to answer the following questions:

- **RQ1:** What socio-technical challenges do Pakistani immigrants encounter in the US?
- **RQ2:** What are Pakistani immigrants' security and privacy perceptions, practices, and needs?
- **RQ3:** How do generational differences influence the perception and prioritization of security and privacy concerns among first- and second-generation Pakistani immigrants? What role do parents and their children play in each other's tech use and safety?

1. * indicates equal contribution.

From these interviews, we identify the following key findings:

1) First-generation Pakistani immigrants encounter several socio-technical challenges, such as language barriers, adapting to advanced technology, discrimination, and online privacy concerns. These challenges are likely shared by other immigrant groups, particularly those from non-English-speaking countries, and Muslim majority countries. These challenges necessitate research and development of technological solutions to help immigrant populations address these issues. Interestingly, second-generation immigrants have quickly adapted to life in the US and do not perceive most of these challenges, a trend that may also be similar in other second-generation immigrant populations.
2) First-generation immigrants' security and privacy perceptions center on their immigrant identity, with concerns about government surveillance, profiling, and physical violence due to their Muslim status. They also fear reputational harm from online content, complicated by differing standards between the US and Pakistan. Based on their threat models [11], they make rational decisions, prioritizing security over convenience. In contrast, second-generation immigrants' security perceptions and practices are largely identical to general perceptions and practices in the US population [11], [12].
3) In Pakistani immigrant families, parents (first-generation immigrants) and children (second-generation immigrants) support each other's technology use. Children often act as tech-support due to their higher tech literacy. We also find that filial piety is significant, as children willingly help out of respect for their parents. Parents' roles in their children's tech usage vary by age: they monitor and mediate younger children's use but trust adult children to manage their own, despite concerns about their security and privacy habits.

Based on our findings, we believe there is substantial room for more research in the area of immigrant security and privacy. First-generation immigrants to the US clearly have different security and privacy perceptions and practices than the general US population. Our findings are likely generalizable to other immigrant groups, especially with regard to socio-technical adaptation and overcoming barriers. As such, there is an urgent need to study a wide range of immigrant populations to understand their unique perceptions, practices, and needs.

From the usable security community, there is a need for developing resources for first-generation immigrants that help them be more aware of and better adapt to new security and privacy practices when transitioning to a new country. Based on our findings, such groups may be more likely than average to adopt security advice and take additional proactive actions to protect their online security and privacy, if they perceive the threat to be likely and severe. Our findings suggest that security experts should adopt tailored education and intervention strategies that respect diverse perspectives and priorities.

Likewise, there is significant potential for research and development of tools to better support first-generation immigrant populations. Social media platforms and other tools need to more carefully consider cultural and religious contexts when designing products. For example, exploring how platforms could allow immigrants to segment what content they share with whom would help them navigate the complexities of interacting with friends and family from two locations with vastly different societal norms and expectations.

2. Background

An immigrant is defined *"from the perspective of the country of arrival"* and is *"a person who moves into a country other than that of his or her nationality or usual residence, so that the country of destination effectively becomes his or her new country of usual residence"* [13]. Migration can be forced, with such migrants labeled as refugees. It can occur through government-sanctioned channels or illicit means (i.e., undocumented immigration). Immigrants bring with them cultural and religious backgrounds and prior experiences with technology, all of which may affect their digital security and privacy in their new country.

2.1. Muslims in America

In this work, we focus on Muslim immigrants to the US. The marginalization and discrimination of Muslims in America, especially after the 9/11 terrorist attacks, have been well-documented in the literature [14], [15]. A recent Pew report reveals that Muslim Americans continue to face negative views and experiences 20 years after 9/11 due to their religion, despite their growing presence in the US [16]. Moreover, Muslims are subject to more scrutiny and surveillance by the state and society [17], [18], [19], which may also have implications for their online behavior.

The label of *Muslim* carries the stigma of *terrorism*, so Muslim Americans often choose either not to reveal their religious identity or present it in a way where it is more matching with Western standards [20]. This situation poses its own set of challenges since such Muslims often encounter criticism from other Muslims due to being perceived as too Westernized. Consequently, these individuals are neither fully embraced as Muslim nor fully accepted as American, leading to the denial of the full benefits associated with either status while simultaneously bearing the burdens of both identities [21]. A study of Muslim-American women finds similar issues; they were concerned about sharing content online that could be considered inappropriate by their cultural or religious communities, such as photos with the opposite gender, alcohol, or revealing clothes [22].

2.2. Security and Privacy in Pakistan

Pakistan is located in South Asia. Pakistan's collectivist society promotes a culture of trust and belongingness, where

privacy is not considered an individual right, and phone sharing is common among family members [23]. A study of 40 Pakistani users found that most were low-literate and were unaware of how to secure their devices or online accounts [24].

Interviews with 73 women from Pakistan showed they largely depended on their male relatives and children to introduce and teach them about technology [25]. This reliance on males primarily stems from religion, where Islam emphasizes gendered family roles with men as the protectors and maintainers of women. Interviews with 34 young Pakistani adults found gendered differences in the experiences and types of harm experienced between young adult men and women, with women mostly concerned about harm to their reputation and men about financial fraud [26].

3. Related Work

3.1. Migrant S&P Perceptions and Practices

A growing body of work has examined the digital security and privacy needs of immigrants to the US. Immigrants are uncomfortable with the amount of information they need to share during the visa process and are vulnerable to scams [8]. Refugees to the US must rely heavily on case managers and teachers for help with technology, which can lead to security and privacy being less of a priority or infeasible [7]. Refugees also struggle with limited technical expertise, language skills, cultural barriers, and scams. Undocumented immigrants in the US have security and privacy behaviors that match that of the broader population, believing the government already has detailed information on them [6].

Outside of the US, migrant domestic workers in the UK, who are often on temporary visas, are concerned about government surveillance, scams, harassment, and employer monitoring [27]. They seek safety in their communities, keep personal details private, and are interested in legal reforms that will allow them to live and work freely. People with migration backgrounds in Germany experience cybercrime at higher rates than other groups [28].

This paper builds upon this nascent body of work by examining the security and privacy perceptions, practices, and challenges of legal, non-refugee Pakistani immigrants to the US. As research into this area is limited, any new data on additional immigrant groups is of immense value. Additionally, our data help fill a knowledge gap, as prior research has focused on undocumented immigrants [6], refugees [7], immigrants to non-US countries [27], [28], or focused on the migration event [10] as opposed to life after immigration. As such, our work provides valuable insights into a legal, non-refugee US immigrant population. Moreover, this is the first security and privacy research specifically targeting a Muslim immigrant population.

3.2. General US S&P Perceptions and Practices

Prior work has shown that US users have a generally lackadaisical attitude towards security [29], [30], [31]. While they are concerned about issues such as viruses, hacking, scams, identity theft, and misinformation [12], [32], [33], they feel that these issues can largely be addressed through personal vigilance [11]. Some users will employ additional protective steps, but only if they have had prior experiences with being attacked [29], [34] or if they feel the task they need to complete is unusually sensitive [11]. In many cases, users will avoid security technologies as they feel the cost of adoption is not worth the security benefit [35], [36].

We find that second-generation Pakistani immigrants closely align with these perceptions and practices. In contrast, first-generation immigrants have concerns that are more closely tied to their immigrant identity. Due to these increased concerns, they are more willing than the general population to sacrifice convenience for security.

3.3. Parent-Child Dynamics

Prior work has explored the role of younger adults in their elders' technology learning [37], [38], [39]. For example, younger family members play the roles of influencers, supporters, protectors, and monitors in older adults' technology learning [10]. They also serve as significant sources of instruction and help for older adults [40]. Studies in cultures that value filial piety have shown that younger family members take it as their responsibility to help their elders in their technology use [10], [41]. A wide body of work has found support from friends and family [42] and grandchildren to be the primary source of help for older adults. [37], [39], [40], [43]. Older adults often delegate their security maintenance to family members or someone in their social circle [44], or someone in the family takes charge of their security and privacy [45].

Prior work has also explored parents' impact on their children's technology usage. The current literature has shown that parents play a role in guiding their children through using technology and the internet, impacting their vulnerability to internet addiction [46], [47], [48], [49], monitoring their kids' online activity [50], [51], [52], and installing content filters [51], [53], [54]. Parents are concerned about dangerous situations that children can encounter online (e.g. [55], [56]), and they are theoretically readily available to help their children avoid such problems. However, the research has also shown that sometimes parents are not aware of what their children are doing online [50], [57] or they are not aware of the best privacy and security practices [58], preventing them from being able to effectively fulfill their role in the parent-child dynamic. Furthermore, parents and children often have mixed attitudes toward content filtering and online surveillance [52], [59], [60], [61], resulting in tension in the parent-child dynamic.

4. Methodology

As Pakistani immigrants in the US are a relatively understudied population, we opted for a qualitative approach in our work. We conducted 25 semi-structured interviews [62] between October 2023 and January 2024.

4.1. Study Design

We directed the participants to our study page that had FAQs about our study, details of eligibility, compensation, the consent form, and the signup link.[2] All interviews were conducted over Zoom[3] and each interview was about 45 minutes long. Each participant received compensation totaling USD $50 as an Amazon gift card. To encourage parent-child participation, we offered an additional USD $25, again as an Amazon gift card, to each participant if they participated as a parent-child pair. In such cases, we conducted individual interviews with each participant, followed by a joint interview lasting up to 10 minutes, if necessary, to better understand their shared stories, and if the participants preferred to share together. To ensure inclusivity beyond English-speaking immigrants, we conducted interviews in Urdu and English, allowing participants to choose their preferred language [63], [64].

At the beginning of each interview, the interviewer presented participants with a study overview, obtained verbal consent for recording, and allowed them to ask any clarifying questions. The interview generally followed our protocol, shown in Appendix A.2, and began with general questions about their technology use and family structure, which we used to contextualize our findings. We then asked about their safety habits, sources of advice, and the advice shared between first- and second-generation immigrants. The third segment explored participants' threat models, specific security practices, and their current safety measures.

Each interview concluded with a debriefing session, during which the interviewer rectified misconceptions, answered questions, and expressed gratitude for the participants' time. Initially, our interview protocol did not incorporate any questions about religion. However, due to the recurring theme of religious aspects observed in the first four interviews, we decided to include relevant questions about religion in our interview guide to comprehensively explore participant perspectives and experiences as Pakistani immigrants.

4.2. Recruitment

We recruited first- and second-generation immigrants to the US from Pakistan. For the purpose of our study, individuals who immigrated with their parents when they were 13 or younger were classified as second-generation immigrants, whereas those who immigrated at 13 or older were classified as first-generation immigrants. All our participants were over 18 years of age. Our exact criteria, as described to the participants, are listed in Appendix A.

Since we wanted to speak with participants residing across the United States, we conducted a thorough search for Facebook groups intended for Pakistanis living in the US. Although we discovered several groups, most were open to the public without vetting procedures, leading to an influx of spam posts within those groups with members from various South Asian countries rather than Pakistan specifically. Consequently, we decided to post our study invitations in a Facebook group exclusively tailored to Pakistani women residing in the United States. We chose this group due to its stringent screening process overseen by group administrators. It is a private group with about 35k members, where membership is restricted solely to individuals referred by existing members. We also recruited through snowball sampling that was iterative until saturation. The responses from the second-generation immigrants were very uniform across the first five interviews. We conducted five more interviews with second-generation immigrants to validate data saturation but found no new themes.

We did not prescreen participants; if they signed up for the study, we believed their assertion that they were eligible. Based on participant responses, we saw no indication that any participant would have been ineligible for the study.

4.3. Demographics

We interviewed 25 Pakistani immigrants living in the US. 15 of them are first-generation immigrants (parents, represented by P), and 10 are second-generation (children, represented by C). 18 were female, and 7 were male. Five were 18-24 years of age, six were 25-34, four were 35-44, four were 45-54, and six were 55-64. In total, there were 17 family groups. However, we do not denote these relationships in Table 1 as that has the potential to deanonymize participants to other members of their family group, given that we used snowball sampling. 10 participants from 6 distinct families were recruited through snowball sampling. The participants were not all from the same extended families and represented 12 different states across the East Coast, South, West, and Midwest.

Pakistan is predominantly Muslim, with Muslims comprising 96% of the population [65]. Within our sample, 23 out of 25 participants identified as Muslim, while the remaining 2 identified as Christians. To guard against re-identification, we refrain from explicitly identifying which two participants in our sample identify as Christians.

Table 1 shows the demographics of participants.

4.4. Data Analysis

We first transcribed the audio recordings to prepare our data for analysis. We manually transcribed the audio recordings if they were in Urdu, with no translation applied. For English interviews, we used Otter.ai.[4] Participants were informed of this during the consent process and consented to its use. We reviewed each transcript for accuracy.

We analyzed our interviews using thematic analysis [66]. First, two researchers, both immigrants from Pakistan (fluent in English and Urdu), collaboratively conducted initial coding, systematically identifying level-one codes while preserving the participants' wording [67]. When necessary,

2. Our supplemental materials are available this link.

3. Our IRB approves Zoom for use in research, whereas other video conferencing platforms are not approved.

4. https://otter.ai/

ID	Age	# of years	Gender	Education Level
P01	38	15	Female	Bachelor's Degree
P02	39	07	Female	Some college
P03	47	24	Female	Master's Degree
C04	21	21	Male	Some college
P05	33	15	Female	Bachelor's Degree
P06	60	13	Male	Master's Degree
C07	30	13	Female	Bachelor's Degree
P08	54	14	Female	Master's Degree
C09	31	13	Male	Master's Degree
P10	44	17	Female	Bachelor's Degree
C11	31	20	Female	High School
P12	61	30	Male	Professional Degree
C13	20	08	Female	Bachelor's Degree
P14	59	30	Female	Professional Degree
C15	24	11	Male	Some college
C16	21	09	Female	Some college
P17	42	16	Female	Master's Degree
P18	62	14	Male	Master's Degree
C19	24	14	Female	Bachelor's Degree
P20	57	12	Female	High school
P21	53	14	Female	Bachelor's Degree
P22	58	06	Male	Master's Degree
C23	28	14	Female	Bachelor's Degree
P24	53	07	Female	Master's Degree
C25	30	20	Female	Master's Degree

In the participant ID, P represents Parent and C represents Child.
TABLE 1. PARTICIPANT DEMOGRAPHICS.

the researchers revisited the audio recordings to clarify content or tone. Second, the researchers grouped similar codes into higher-level concepts. Finally, the researchers identified themes by connecting these concepts and delineating the overarching themes discussed in our findings. In this final step, all authors participated in analyzing the data and extracting relevant themes. Throughout the process, we took detailed coding notes and memos.

We conducted our coding iteratively in lock-step with the interview process. This allowed the researchers to continually assess saturation and adapt the interviews as new themes emerged. Ultimately, we only added a single line of inquiry about how participants felt their Muslim faith related to their security and privacy perceptions, practices, and needs.

As our research is qualitative, we refrain from using precise numbers. Instead, we adopt consistent terminology to express the relative frequency of major themes, following the approach used in previous studies [68], [69], [70]. In Figure 1, we present the terms employed to indicate the frequency of participants' responses.

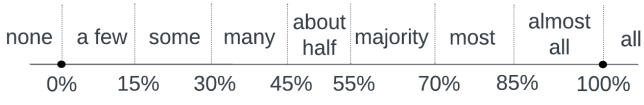

Figure 1. Terminology used to convey relative frequency of themes

4.5. Ethics

Our study was approved by our institutions' IRBs. We obtained informed consent from participants and did not record the video for any of the interviews. Participants were explicitly informed of their ability to skip any questions without affecting compensation. Two participants chose not to respond to the question about how they store their personal information.

4.6. Researcher Positionality

A researcher's identity and positionality influence their choice of processes and interpretation of results [71]. Our team consists of insider and outsider perspectives, helping provide a more holistic view of our results [72]. Two authors immigrated to the US from Pakistan as young adults, one male and one female. These researchers conducted the interviews, allowing the interviews to be conducted in either Urdu or English. Sharing an ethnic and cultural background with the interviewer may have also encouraged participants to share more personal details about their experiences. These researchers were also responsible for the initial coding of interview transcripts, which allowed them to discern the cultural context of participant answers. Two other researchers immigrated to the US from Egypt, one as a young child and one as a young adult. The second-generation immigrant researcher helped develop the interview questions exploring inter-generational interactions, providing valuable insight. Three of the above researchers (two female, one male) are Muslims, which helps provide insights into participants' answers regarding their faith. Finally, two researchers are lifelong US citizens, which allows them to compare immigrant experiences with their own experiences and identify points of similarity and difference.

4.7. Research Context

Our interviews occurred during the Israeli-Palestinian conflict, which has been ongoing for decades. Notably, many of the interviews occurred during the Israel-Hamas war, which escalated after the 7 October 2023 attack by Hamas on southern Israel. In the last three months of the year, the Council on American-Islamic Relations (CAIR) reported a 178 percent increase in requests for help and reports of bias compared to the previous year [73]. CAIR indicated that the rise in Islamophobia was the worst they had seen in 10 years and that complaints included employment discrimination, hate crimes, and education discrimination. CAIR also tracked publicly reported incidents, which included one murder, two attempted murders, and various other incidents of violence and threats of violence toward Muslims.

Due to this context, it is possible that participants were more focused on security and privacy concerns related to their Muslim faith than they normally would be. In particular, a majority of participants noted that they felt uncomfortable commenting on the war on their social media, as they felt it might lead to discrimination or reprisal based on their views.

4.8. Limitations

Although our sample is diverse in terms of age and duration of residence in the US, we cannot claim that it is

representative of the broader Pakistani immigrant population. First, our sample is very small compared to the overall Pakistani immigrant population in the US. Second, our results skew female, potentially failing to identify some male-specific topics and over-emphasizing female-specific topics. Third, our sample was recruited using Facebook and snowball sampling, which may have led to an overly homogeneous population.

Regarding data quality, we note that while having Pakistani immigrant interviewers may have made it more likely for some participants to disclose deeper details, it may also have introduced social desirability bias. Participants were also asked to remember details that may have occurred many years in the past (e.g., parent-child interactions).

Due to these limitations, we stress that our results should not be taken as definitive but rather as exploratory findings. Future research will be needed to quantify the prevalence of topics identified in our qualitative research.

5. Findings: Socio-Technical Challenges

We now move to discussing the findings from our research, beginning with socio-technical challenges faced by our participants as Pakistani immigrants living in the US. While many of these do not have a direct security and privacy connection, understanding this background will be helpful as researchers build technology looking to assist this immigrant population.

5.1. First-Generation Immigrants

We noticed that our participants did not have a clear distinction between challenges encountered in offline and online settings. Their behaviors and experiences offline appeared to significantly influence their online behaviors and patterns. In this section, we aim to illustrate these issues, which help contextualize the decisions and security practices of our participants.

5.1.1. Navigating new technologies. Many of our participants shared that when they first came to the US, they encountered a significantly more advanced technological environment than what they were used to. They reported feeling "*unprepared*" (P14) and "*stupid*" (P5) for their lack of technical knowledge. They recounted instances where they struggled with basic tasks, such as navigating credit card portals or finding themselves unprepared for the advanced technologies present in their workplaces. P22 elaborated on the technological difficulties he faced when dealing with automated systems in the US, as there are usually human operators in Pakistani offices:

> "*Most of the problems I faced were with the automated systems. In whichever office I would call they would have an automated answering machine installed. It was confusing to understand [the automated voice] unless an operator intervened. In many offices they do not even have an operator so I face difficulties communicating there.*" (P22)

Similar to refugees [7], immigrants with less experience with technology focused more on their primary goals with the technology, rather than learning how to use it securely and privately. Before arriving in the US, some participants mentioned they did not know how to type on a keyboard. The necessity to learn and adapt to technology overshadowed their immediate attention to any security or privacy aspects. P14, who worked as a medical doctor at the time, mentioned:

> "*At that time I was not even worried about how to be safe or anything. I just wanted to learn [typing] so I could do my job.*" (P14)

5.1.2. Communication barriers. The participants' proficiency in English played a pivotal role in their acculturation process. Familiarity with the language facilitated integration, while a lack of it contributed to stress (P8), feelings of inadequacy (P10), and diminished self-esteem (P5), leading to difficulties in using technology effectively and seeking help. These linguistic barriers increased their susceptibility to technological harm, aligning with findings by prior work with non-native speakers identifying phishing emails [74] and with refugees [7]. Some participants mentioned that interacting within the community posed challenges as well because they struggled to comprehend the American accent and the fast pace of speech. P8, for example, said:

> "*They used to talk very quickly, so I would constantly tell them please slow down, I cannot understand you, slow down. So if I had gotten a little bit of training on this, it would have been immensely helpful.*" (P8)

Many participants shared experiences where their accents posed challenges in being understood, both by local individuals and technology. For instance, P12 stated:

> "*Siri can't understand my accent no matter how much I try.*" (P12)

Moreover, participants recounted situations where biases were quickly triggered due to their accents. Such experiences acted as an additional barrier, hindering their ability and opportunities to gain tech literacy. P24 mentioned:

> "*Anytime I call somebody [for support], when they hear this accent, the first thing is that [their] implicit bias kicks in...in their head, it's the dumb foreigner.*" (P24)

5.1.3. Lack of social support. Upon immigrating to the US, which has its own culture and norms that are vastly different from those of Pakistan, immigrants often lose the family support and social ties they had back home. This often leads to a heightened risk of isolation and increased distress among immigrants. P8 shared that upon arrival, her nervousness and stress made it more challenging for her to learn new technologies.

> "*I think it was harder for me to learn as I was nervous...because it was the first time we were alone...we didn't have any family support. We had nothing here, no friends...and it was a totally new country...so, I felt a lot of stress when I moved here because of all these things.*" (P8)

5.1.4. Discrimination. The majority of our participants mentioned facing discrimination in some form, either online or in their daily lives. They shared that revealing their identities online made it tougher for them to make friends or secure jobs as people immediately held biases against them. Additionally, they recounted instances where they experienced racism, with individuals telling them to "*go back home.*"

> "*Even last week I was told to go back to my country, which...I've been living here [in the US] for 31 years now.*" (P14)

Such incidents made our participants afraid of expressing themselves online because they realized that anything they said could be taken the wrong way due to their identity, so they refrained from talking about anything sensitive, particularly religion and politics. P24 said:

> "*If I was white, or if I was black, I would be just another American talking something about politics, but when they see a Pakistani or Muslim say something, it is not accepted as just a view. It is accepted as if I'm representing the Taliban community.* " (P24)

Almost all of our participants, being Muslim, emphasized the threat of religious-based harassment in both online and offline contexts. They had either experienced Islamophobia firsthand or knew someone who had. They often encountered anti-Islam content on social media but chose not to engage, fearing potential backlash. Among the variety of incidents our participants described, one shared by P8 stands out. P8, who wears a hijab, posted a simple "I agree" on a neighborhood forum discussing a rude neighbor. Subsequently, she received a threatening message accusing her of being a terrorist solely due to her hijab, which led her to involve the police. Following this incident, she refrained from expressing her views online again, as advised by her children.

We found that while race and religion impacted the experiences of Pakistani immigrants, these experiences also varied with gender. As such, looking at these factors independently is insufficient because these social positions are experienced simultaneously. Our findings suggest that many women have experienced discrimination more frequently and more intensely compared to men in our sample. For example, two participants, husband and wife, immigrated to the US together and lived together in the same place. They both had the same profession at the same seniority level. Still, the wife highlighted several instances of discrimination based on her identity as a brown Muslim female. She recounted situations where clients explicitly asked for a *male* professional or expressed a reluctance to engage with a professional who shared her specific attributes. The husband however did not face such incidents of discrimination at his workplace and feels well-respected.

5.1.5. Self-presentation and expression. About half of our participants faced challenges in upholding their online privacy boundaries, particularly on social media platforms. They struggled to balance their identities, having friends from both Pakistan and the US, as their desired presentations often conflicted, potentially resulting in context-collapse [75]. Many participants shared that they refrained from posting pictures with their US friends or sharing aspects of their American lives on social media. Doing so might cause discomfort among their relatives in Pakistan, who might not experience a similar lifestyle, leading to feelings of discontent, and causing problems in their relationships. P8 highlighted this, saying:

> "*The thing is, those people say, 'Oh, she's having a good life,' and all. I mean, I feel like maybe they don't have [this lifestyle], but I do, so I don't want to give them that kind of image. They are my relatives; I want to maintain good relations.*" (P8)

While most of our participants stated that they do not post about their religious views online due to being afraid of religious extremism and anti-Islam narratives, a few stated that their religious views diverge from prevailing Pakistani norms so they feared that expressing these views might offend people in Pakistan instead, potentially eliciting strong reactions from religious extremists in Pakistan. Describing this issue, P12 said:

> "*I'm more afraid of posting in Pakistani groups because my religious views are against 99.9% of people there. So, I'm more worried that if I post something there and I'm traveling to Pakistan, it's probable that some extremist's religious sentiments get stirred up, and they may attack me. So I'm scared when posting anything.*" (P12)

5.2. Second-Generation Immigrants

While first-generation immigrants highlighted various challenges they encountered, interestingly, such incidents were relatively rare among the second generation. This disparity may be attributed to the fact that second-generation immigrants have established support systems and benefit from their parents' efforts in building communities. Additionally, second-generation immigrants also reported minimal experiences of discrimination, suggesting that they have acclimated to the language and culture in the US.

The only challenge that second-generation participants mentioned was navigating the blend of cultural expectations between their Pakistani families and the US culture. For instance, C16 refrains from uploading photos online, despite not fully grasping why posting a photo is discouraged, especially when her American friends do so without concerns.

> "*My account is private, and I only have, like, my friends on it, who also post their photos. But I think they [parents] just want to protect us. They're like, 'Oh, they're girls and they're just gonna get out of hand.' They think once you start putting modest pictures you might later just post random indecent ones. You know how Pakistani parents are*" (C16)

Additionally, participants expressed feeling that their parents impose stricter rules and monitor their activities more closely compared to their friends' parents.

> "*They were a little heavier on monitoring what I was doing, and whether or not I was safe...they were themselves very cautious. And they were cautious for me too.*" (C15)

6. Findings: Threat Models

Participants' security and privacy perceptions and practices were influenced by personal experiences, shaping distinct perspectives for parents and children. Parents predominantly perceived targeted threats linked to their identity, while children perceived broader, generic threats that could affect anyone. We broadly asked them what threats they perceive to their online safety and the measures they take to protect themselves against those threats. We now describe these threats, their consequences, mitigation strategies employed, and sources of information as described by our participants.

6.1. First-Generation Immigrants

The concerns of first-generation immigrants predominantly arose from their real-world experiences. They then projected these experiences into their perceptions of potential online threats. In this section, we outline some of the most common threats perceived by our participants.

6.1.1. Government surveillance. Almost all of the parents in our study expressed a perception of government surveillance, convinced that they are subjected to continuous monitoring and comprehensive data collection on every aspect of their lives due to their identities. P12 shared his concerns, saying:

> "*Being a Pakistani Muslim, I come to the conclusion that my phone and my communication is recorded 100% of the time. It's not ifs and buts*" (P12)

The consequences described mainly involved having a pervasive sense of surveillance and being under scrutiny, notably having the fear that their words could be misconstrued or taken out of context. Additionally, they expressed concerns that their statements, even in jest, might be documented which could adversely impact their applications for a green card or US citizenship. They also worried about losing their jobs because of any controversies stemming from these statements. A few participants referred to recent incidents at Harvard where students expressing their views on the Israel-Palestine war had job offers rescinded and organized efforts were made to keep them from any future employment [76]. Participants emphasized their desire to avoid similar situations. However, some participants mentioned that despite their general avoidance of posting about religion, they do express support for Muslims in Gaza, considering it an important cause, regardless of potential adverse consequences.

Mitigations: Participants perceived this threat as highly likely. To protect against the consequences, our participants mentioned that they avoid posting online about religious or political views, or any other topic they think is sensitive. On their social media platforms, many participants chose to be passive observers rather than active participators, a behavior also mirrored in other exposure-sensitive populations [77]. Some participants expressed their reluctance to even share examples of topics they avoided discussing online, fearing that those topics might contain buzzwords that could attract unwanted attention from the government. They felt that they had to censor themselves to avoid being targeted or discriminated against because of their identities. They mentioned that they are "*walking on eggshells*" (P3) because of their status in the country.

6.1.2. Physical threats. Most of the participants were genuinely worried about physical harm, fearing that extremists might target them through hate crimes.

> "*People here can sometimes be crazy, you can't predict their actions...and their actions could affect you very badly, so I always advise my kids to keep yourself safe because you don't know.*" (P8)

They were concerned about the potential fallout from posting something online that might offend someone, leading to that person stalking and possibly causing them physical harm merely due to an opinion shared online. They also pointed out that the way Muslims are portrayed negatively in the media has greatly harmed their image, putting them at higher risk of becoming victims of hate crimes.

Mitigations: Participants outlined various mitigative measures to stay safe from such threats, primarily centered around abstaining from engaging in discussions or arguments, both online and offline. Parents particularly mentioned that they advise their children to exhibit exemplary behavior in classrooms, emphasize kindness, and teach their children to portray a positive image of Muslims through their actions. They encouraged their children to be considerate to everyone around them.

> "*I repeatedly tell my kids to be kind to others and stand up for people being bullied in school, and we have done that in the past.*" (P5)

6.1.3. Apps collecting data for profiling. Almost all participants said that they were aware of the apps collecting data on every single aspect of their lives. A few participants particularly mentioned Facebook, stating that it collects the kind of data it doesn't really need to function. They said

the multitude of apps makes it impossible to pinpoint which ones are collecting which data. Then, this data is then just sold to third parties without the user's consent and is maybe even used for racial profiling.

> "*There are so many apps on my phone, there is no way I can keep tab which are the apps which are actually recording.*" (P12)

Mitigations: Most participants expressed a sense of resignation regarding apps collecting data about them, noting that they feel limited in their ability to control the situation. Some mentioned attempting to adjust app settings and restrict permissions but found it challenging as settings often revert with each app update.

6.1.4. Reputational harm. Some participants mentioned that with AI becoming more common there is now elevated risks of harm. They mentioned deepfakes and worried about loss of reputation due to deepfakes. For this threat though, participants mentioned that they only worry about their daughters and female family members, as they did not think that anyone would target a male family member for deepfakes.

Mitigations: The mitigation for this type of attack was purely offline, mainly consisting of being modest and wearing a hijab (head-covering worn by many Muslim women). P17, for example, said:

> "*Depends upon who it is. Like if it is a daughter then it's about her honor...and I think the hijab I wear might prevent deepfake to some extent... I think that there are some things that can't be done because of hijab.*" (P17)

Some of our female participants mentioned that they do not put pictures of themselves online, and advise their daughters to not do so either, but that was not linked to fear of deepfakes, but rather generally for modesty since it is culturally preferred for women to not have their pictures online. This is not something we found within or for male participants. For them, the concern majorly was financial, consistent with the findings of [26] in Pakistan.

6.1.5. Financial threats. Most of our participants mentioned some sort of financial threat. Financial harm is something that participants, especially in their beginning years in the US, can't afford because they don't have any family support to fall back on. Participants mentioned hacking, social engineering attacks, scams, and phishing. Participants mentioned being particularly suspicious of Shein and Temu since they had heard negative reviews about the financial security by these companies. A few participants also mentioned not using their credit cards when shopping on smaller vendors since their security cannot be trusted.

Only two participants mentioned identity theft as a concern — one had personally experienced it, while the other's brother had fallen victim. Apart from these instances, most participants did not perceive identity theft as a threat.

Mitigations: To protect themselves against financial threats, our participants mentioned a wide variety of mitigations. Some of them include enabling two-factor authentication (usually through a text message to receive a one-time PIN), refraining from saving credit card information on websites, deleting apps with a history of security breaches, avoiding the use of credit cards in smaller vendor stores, closing all other apps while banking, and opting out of mobile banking altogether.

6.1.6. Threats from posting online. Almost all of our participants were cautious about what they posted online. They believed that posting content online could lead to various harms. They identified relational harm as a primary concern, fearing negative reactions from friends and family if they were to post certain content online that their social circles may disapprove of. Additionally, participants expressed concerns about the possibility of inviting the "*evil eye*" by sharing pictures online, particularly if others might envy their lifestyle. This belief is rooted in Muslim traditions, where it is believed that an evil or envious glance may have the potential to inflict injury, harm, and even death to those upon whom it falls [78]. Participants mentioned refraining from posting pictures with their friends in the US or sharing details about their life there because they were concerned it would make their relatives in Pakistan feel bad. A few participants also expressed concerns about the potential risks of posting their location online. For instance, P3 shared an experience where she posted about being on vacation, only to return home and find that their house had been robbed while they were away. She considered the burglary to be directly linked to her announcement of being away on vacation.

> "*I was a heavy user of Facebook, and I think I posted a picture, like, we're going here, and then two days later, we had a robbery at our house, you know. So, based on that, I think maybe people knew that I wasn't at home or whatnot. So, I have actually stopped sharing that type of content, like where I am going and all.*" (P3)

A few participants mentioned the possibility of hacking, suggesting that if someone dislikes something you post online, they might attempt to hack into your accounts.

Mitigations: To protect themselves, participants primarily opted to maintain a low profile on social media. Rather than engaging actively, many chose to be passive observers. They refrained from posting about their vacations in real time and avoided sharing their current locations or check-ins. Instead, they posted about their vacations after returning.

6.2. Second-Generation Immigrants

Unlike the first-generation, second-generation immigrants did not perceive themselves to be particularly vulnerable due to their specific identities. They also did not believe that they were necessarily at greater risk compared to their non-immigrant friends. Their perceived threats were more generalized internet crimes that could happen to anyone. The mitigations they employed were generally more technical compared to those of the first generation.

6.2.1. Scams and identity theft. Participants highlighted the prevalence of online scams and identity theft as significant threats on the internet. They expressed concerns about the increasing difficulty of protecting oneself due to the wide variety of such scams out there. Specifically, participants were worried about scams that attempt to obtain the victim's social security number, as this could lead to identity theft and severe consequences. C19 describes the consequences of such threats as:

> "*Um, so like, it could like ruin your life in any aspect, basically, like, you could lose your job, your private information, you lose the passwords to everything, which will also affect your financial information. But you could lose your... everything could go in like the blink of an eye, if you just like fall for these scams.*" (P19)

Mitigations: To mitigate the risk of scams, participants mentioned that they exercised caution when storing or sharing personal information. They mentioned avoiding untrustworthy websites and refraining from sharing their social security details with anyone. Rather than storing this information, they memorized and used it as needed. They also took additional proactive measures such as blocking suspicious phone calls and not clicking on unknown links. Their self-efficacy was high, meaning that they mostly felt confident that they were equipped enough to identify scams and effectively protect themselves.

6.2.2. Hacking and data breaches. A few participants mentioned hacking and data breaches as a prevalent threat to their online safety and privacy. Data breaches can make their personal information public which they felt a concern for. However, they did not think that someone would specifically target them and hack their accounts. Rather, they worried about the mass data breaches that happen, which "*could happen to anyone*" (C4)

> "*To me personally? No. I don't think anyone's out to get me or anything. I think the only attacks I [would] be at a risk for is when there's like massive data leaks from the different websites and stuff. But yeah, I think that's it.*" (C19)

Mitigations: The mitigations mentioned for this type of threat mainly included keeping stronger passwords and not reusing them. Specifically, for banking websites, they emphasized using passwords that significantly differ in pattern from all other passwords. As for mass data breaches, participants said that they could only protect themselves to a certain extent.

6.2.3. Fake news and misinformation. Some participants also expressed concern about the abundance of information on the internet, noting that a lot of it is actually fake or wrong. They also stated that it is becoming increasingly difficult to filter out incorrect information. The consequences of believing in misinformation can range from becoming more vulnerable to scams, to developing prejudiced extremist views. They mentioned encountering a significant amount of misinformation on social media recently regarding the Israel-Palestine conflict.

Mitigations: The participants expressed skepticism and stated that they were cautious about believing everything they encountered on the internet. They highlighted this as a threat that their parents might be more vulnerable to, implying that older generations may be more inclined to trust the information they find online without verifying its accuracy.

6.3. Educational Resources

We studied where parents and their children learn about internet safety. We saw that parents learned haphazardly either through experience, hearsay at workplaces, or their children. For instance, P17 had heard that GroupMe, a group texting app, is less secure, so she was concerned about using it, but she had not verified this information or obtained further details of why it might be less secure. While community-based learning served as a significant resource, the information was often imposed without a clear rationale communicated. This sometimes left participants fearful of a certain app or action without understanding the underlying reasons.

Our participants had no access to formal resources for learning how to protect themselves online or understanding potential threats. Their knowledge about internet safety was acquired in an ad-hoc manner, often on the go. For many first-generation immigrant women in our study, their husbands served as a primary source of information about internet safety. However, men in the study did not cite their wives as significant sources of information on internet safety. Instead, they tended to rely more on external sources, such as their workplaces or friends.

Children similarly mostly learned through trial-and-error, primarily from the internet and discussions with friends. Some participants recalled attending media literacy lectures in their schools during their younger years, where they learned about basic safety rules such as not talking to strangers or sharing passwords. However, currently, they mainly rely on Google and their friends. All participants mentioned that they do not seek guidance from their parents to learn about internet safety, as their parents have limited knowledge in this area.

7. Findings: Parent-Child Dynamics

In our study, we aimed to explore the inter-generational family dynamics concerning technology usage, specifically exploring how children assist their parents in navigating the digital landscape and vice versa. Our findings indicate that cultural norms and beliefs are deeply intertwined with the parent-child dynamics, shaping how parents interact with their children, the aspects of technology they control, and how children perceive these interactions. We also describe their device-sharing practices and mutual perceptions about their digital safety hygiene. Future work could explore the

extent to which other populations share similarities or exhibit differences in these culturally-influenced dynamics.

7.1. Role of Children in Parents' Tech Usage

Our study findings are consistent with those of Tang et al., who found that younger adults played the roles of supporters, influencers, and protectors in assisting their elders with technology use [10]. In our study, we observed that children, benefiting from better tech literacy and education in American schools, primarily assumed the role of supporters, where they assisted their parents in their technology use. Their support included tasks such as projecting videos on TVs (P17), setting up new devices (P5, P3), adjusting settings on Facebook (P8), and troubleshooting device issues (P10). At times, children even created written step-by-step instructions for tasks perceived as complex by their parents, which the parents later referenced as guides. Overall, we heard unanimously from all parents and children that the children were eager and willing to assist their parents. This conduct also stemmed from a strong cultural norm of "*filial piety*" in Pakistani families, where children perceive it as their duty to support their aging parents as a gesture of gratitude for their past care and support. The sense of duty, reverence, and support toward parents and older family members is considered customary by children and is expected by the parents. This parallels findings observed in other Asian cultures, such as China [10].

Children also sometimes played the role of influencers [10], encouraging their parents to create social media accounts, use two-factor authentication, and set strong passwords. Some participants noted that their children regularly warned them about scams, data breaches, and misinformation on platforms like YouTube or social media, frequently advising: *"don't believe everything that's on the internet."* (P8)

While prior studies suggested that older adults often preferred independent learning rather than seeking help from family members [79], [80], our findings differed. We observed that participants in our study were quite willing to learn from their children and were open to their guidance. Whether it involved adopting new technologies, receiving security advice, or having their children set up devices for them, almost all parents referred to their children as "*their main IT folks*" (P17, P2). This trend remained consistent regardless of their children's age, whether they were in their teens or thirties.

7.2. Role of Parents in Children's Tech Usage

We noticed a significant variation in the role of parents in children's tech use based on the children's age. Concerning younger kids and teenagers (under 18), parents tended to actively mediate their children's technology use. This monitoring encompassed several aspects, including time restrictions — defining specific time slots for device usage, and content restrictions — determining what type of content their children could access or share online, with measures like installing YouTube Kids on their devices. Additionally, parents monitored and tracked their kids' online activities, occasionally checking their browsing history or physically examining their phones. They also supervised and regulated their children's social interactions online, including who they could communicate with or engage with online. Some parents also monitored their children's live location by using location tracking apps like Life360.

Parents of younger children often struggled to balance technology mediation with appropriate strictness. Their children found their friends' American parents to be less strict, creating tension between Pakistani values and the U.S. cultural environment. Despite limited exposure to their cultural heritage, children typically complied with their parents' rules out of respect, understanding these expectations were shaped by cultural values. For example, C13 said:

> "*So I don't truly understand the reason why [my mother] says the things she does, but I kind of understand where she comes from so I listen to her and don't [post pictures]*" (C13)

For grown children (18 years and older), parents believed they had imparted enough *"tarbiyat"* (upbringing or nurturing) for their kids to distinguish right from wrong. At this stage, parents held a significant level of *"aitmaad"* (trust) in their children. In Pakistani culture, there is a common belief that once children grow older, they will become a source of support for their parents. Therefore, with grown children, the parents expect support from their children rather than trying to actively support or monitor their technology use.

7.3. Device and Password Sharing

We noticed that device and password sharing was common in almost all households among our participants. Most of our female participants mentioned that the passwords to their devices were shared among their husbands as well as children. However, husbands typically maintained a higher level of privacy and shared their devices, at most, solely with their wives and sometimes not even with them. In cases where devices were shared between spouses, each individual had their own device, occasionally using the other's device and having access to all the information on it. Some women mentioned that they do not have access to their husband's phones or laptops because they have "*work stuff*" (P8) on them. We observed an interesting distinction in perceptions of device sharing between husbands and wives. When asked, most women indicated that they did not consider their devices shared with their husbands, even in instances where the husband had access to the device. From their perspective, device sharing was contingent upon the husband *using the device regularly*, rather than merely having access to it. Conversely, when husbands were asked about sharing devices with their wives, they considered the device shared if the wife had the password to their devices. So they defined device sharing as the wife also having *access* to the phone, even if she never uses the device.

We also noticed that the siblings never share the devices, unless it is the mother's device that everyone is using. Sharing among siblings with their parents occurred only when the children were younger. Because of South Asian cultural norms around device sharing [81], [82], [83], all participants reported that device sharing does not affect their use or utility of the device.

7.4. Perceptions of Safety Habits

7.4.1. Parents' perceptions. Regardless of their children's ages, parents unanimously agreed that their kids had more extensive knowledge about technology than they do. They often turned to their children for technology advice, including guidance about security and privacy. However, when questioned about who employed better safety practices on the internet, all the parents asserted that they practiced better safety measures compared to their children.

All of our participants perceived their kids to be reckless and careless when it came to protecting themselves online. Despite acknowledging their lesser technical expertise compared to their kids, parents monitored their children's online activities when they were younger. Even with adult children, parents expressed concerns about their safety behaviors. They recalled instances where their children did not lock the smart home devices upon leaving, displayed carelessness while managing their online banking transactions, and posted online about everything without considering the consequences. Moreover, parents noted that their children might sometimes view them as overly cautious and paranoid, resulting in less receptiveness to their advice. In contrast, parents perceived themselves to be highly receptive to their children's advice.

7.4.2. Children's perceptions. The children viewed themselves as more technologically adept compared to their parents. They regarded their own practices as safer and more cautious and their parents' habits as unsafe, based on their belief that their parents lacked sufficient tech knowledge and were set in their old ways. They pointed out that their parents were more susceptible to scams, often needing guidance to update and strengthen their passwords.

The children did not consider themselves highly receptive to their parents' advice because of having more knowledge about technology. Conversely, they agreed that their parents were quite receptive to the advice given by their children.

> "*Parents can more easily fall victim to scams. They try to learn, but they are not as tech-savvy. They only know whatever we tell them [about technology].*" (C13)

7.4.3. The apparent disconnect. The disconnect between the children viewing their parents as more vulnerable and the parents perceiving their children as more at-risk stems from their distinct perceived threat models. The parents did not consider scams and general technology-related issues to be the most important threats to protect against. Instead, they perceived individualized attacks and certain behaviors as inviting potential problems. They noticed these issues more in their children than in themselves. Conversely, the children focused on broader and more generic threats, leading them to believe their parents were more likely to be at risk. Each group protects themselves against the threats that they believe are more pressing, leading them to feel that their practices are safer than those of the other group.

8. Implications and Recommendations

While our findings are specific to our participants—Pakistani immigrants— we acknowledge that these insights may reflect broader experiences shared by other immigrant groups, particularly those from Muslim or Southeast Asian backgrounds. Below, we present insights and recommendations from our study that aim to enhance the security and privacy experiences of Muslim immigrants, general immigrant communities, and potentially the broader U.S. population. While we believe these generalizations are likely valid, future work is needed to conduct deeper investigations to confirm and better understand the broader implications of these issues.

In line with prior work, we emphasize the need for technology with better privacy guarantees and awareness in users about the security and privacy features of existing technologies [69], [84].

Participants consider cost-benefit tradeoffs when making security decisions. Our findings show that participants make *rational* decisions, meaning they take informed and intentional actions based on their perceived threats and risk assessments [11]. Unlike undocumented immigrants [6] and general findings on privacy practices [35], [36], our first-generation immigrants actively take mitigating steps online to protect against their perceived threats. Contrary to the expectation that individuals prioritize convenience over security [85], [86], our participants showed a willingness to prioritize security even at the expense of convenience or self-expression when they perceive a threat to be severe or likely enough and believe that the protection action would effectively protect them (Section 6.1). This behavior reflects the role of risk perception [87] in security behavior, where the perceived threat severity and likelihood, as well as response efficacy [88] heavily influence participants' decisions about adopting security and privacy-preserving behaviors. This highlights the need for considering subjective risk perceptions and offline contexts when guiding security and privacy behaviors.

Recommendations: We advocate for security experts to consider tailored approaches to security education and intervention strategies that acknowledge the diverse perspectives and priorities of the target populations. Further, we encourage researchers to conduct holistic and in-depth investigations into users' threat models to better understand the rationales behind their security decisions, their threat perceptions, and the barriers they face in maintaining safety. Since non-immigrant populations also make security decisions based on their cost-benefit analyses [35], [36], designing interventions that align more closely with these varied threat perceptions

could improve security outcomes across a broader range of communities, not limited to immigrants.

Participants religious and cultural ideologies impact their security and privacy practices. Aligning with prior work, we find that female participants (whether first- or second-generation) uphold familial expectations of modesty [22], [89], [90], [91] and are careful when posting pictures online. Prior work has also shown that religious values heavily influence how people view privacy [24], [81]. Our participants, for example, refrain from sharing their faces or posting pictures online not out of concern for privacy, but rather out of a desire to uphold the modesty and values practiced by their family (Section 5.2, 6.1.4). Similarly, we recognized the influence of collectivist mindsets, particularly among first-generation populations, where family well-being is prioritized over individual concerns, a norm common in Eastern cultures [23], [92]. Leveraging this collective mindset in designs can be effective, as users may perceive harm to any family member as detrimental to the entire family unit.

Recommendations: We advocate for technology designers and developers to incorporate these analogies and ideologies into design as a powerful way to enhance understanding and create deeper motivations for secure behaviors. We advocate for user-centered designs for such issues to help reframe the alien concepts of privacy and security to familiar concepts using culturally resonant analogies. For instance, reframing the act of not posting a photo solely for privacy gains to a practice that protects modesty may increase the likelihood that users take recommended protective measures. Similarly, designers could also leverage collectivist values to foster communal responsibility in digital interactions, which can be effective for Pakistani immigrants and other cultures valuing modesty, family honor, or collective well-being, such as in Asia and the Middle East [10], [93], [94], [95]. Incorporating these diverse perspectives and cultural insights can enrich technology design, ensuring solutions that resonate with the lived experiences and beliefs of a broader range of users.

However, such approaches present their own set of challenges. One significant concern is the potential for the misuse or exploitation of cultural metaphors in design. If not implemented carefully, technology may inadvertently limit the agency of users by manipulating them to adhere to specific security measures by using cultural or religious beliefs. To avoid misuse, designers must engage with community leaders and members to ensure that cultural metaphors are used respectfully and ethically.

Participants lack access to resources about digital-safety. When immigrant populations initially arrive in the US, they often lack access to formal training programs for tech literacy, as well as knowledge about safety measures, such as protection from scams, and other essential skills common among US citizens. Our results indicate that first-generation immigrants learned about online safety haphazardly through trial and error (Section 5.1). They specifically lacked accessible resources for quick help with tasks such as setting up two-factor authentication or configuring privacy settings on Facebook, which are usually taught incidentally or as part of broader tutorials. Moreover, our participants, like other immigrants [6], have expressed a preference for in-person learning experiences, since they also help with the integration of these immigrants in the society.

Recommendations: Establishing informal structures for learning, such as community-based initiatives, could facilitate a better understanding of common scams and other threats prevalent in their local areas. Such initiatives not only enhance learning but also help build a supportive network that can prevent individuals from feeling isolated. Community centers, libraries, and local non-profit organizations can serve as ideal venues for these programs, providing a familiar and trusted environment for learning. Similarly, creating short, accessible video tutorials—similar to Instagram reels or YouTube shorts—on foundational topics such as setting up two-factor authentication and configuring privacy settings could be particularly beneficial in addressing resource gaps, especially if they offer language support.

Recognizing that teaching technology alone is insufficient due to language barriers, we also recommend providing resources for learning and practicing language skills. While teaching about technology does help, users often, due to language barriers, cannot transfer that information to another technology that has a different interface, even if the other technology is conceptually similar. Providing resources for learning and practicing language could empower individuals to acquire technological skills more independently and efficiently.

Participants are motivated by filial piety. The collaborative dynamic observed in Pakistani families, where children assist parents with technology, hints at the potential for similar intergenerational cooperation in American households. Prior work across domains, such as healthcare and psychology, has hinted at the existence of filial piety within Western cultures [96], [97], suggesting a foundation upon which similar technological collaborations can be built.

Recommendations: Future research in the context of technology may offer valuable insights into leveraging this dynamic to foster a collaborative approach aimed at achieving a better security posture in Western contexts. By acknowledging the significance of filial piety, American families may cultivate environments where mutual learning and support thrive. Researchers should explore how intergenerational cooperation can be harnessed to enhance digital literacy and security practices. This involves studying how children can effectively teach their parents about digital safety and privacy, and identifying the barriers and facilitators to such learning exchanges.

Technology designers should consider incorporating features that encourage family participation and shared responsibility for online safety. For instance, applications could include family dashboards that display recommended tutorials and security tasks, allowing family members to suggest these resources to one another.

Participants struggle to manage multiple facets of their identity. Our participants encountered challenges in regu-

lating their online boundaries and managing their identities due to differences in preferences between their Pakistani and American social circles (Section 5.1.5). This led to self-censorship and a violation of expressive privacy, defined by DeCew as "*[the right of] expressing one's self-identity or personhood*" [98]. The complexity of maintaining multifaceted identities across different social groups or roles is observed in other contexts as well [99], [100]. Our participants mentioned that they preferred WhatsApp groups because they had better separations and the audiences were clear. While Facebook also provides options for tailored audiences, our participants often struggled to understand those and made frequent errors.

Recommendations: Designs that acknowledge users' multiple identities can be beneficial for addressing such challenges. Self-censorship among participants and their reluctance to share content underscores the necessity for social media designers to create platforms that facilitate the management of multiple social roles or profiles. We broadly suggest that tools consider the multiple identities of individuals, and may be built to support: (1) segmented profiles, enabling users to maintain distinct identities for various social circles with separate privacy settings and content; (2) the ability to adjust privacy settings based on different social groups, allowing for tailored control over content visibility; and (3) prompt users to consider audience and context before posting, minimizing the risk of sharing sensitive information with the wrong group, and enhancing user privacy awareness. Such features would likely benefit not only immigrants but also other groups facing similar challenges of context collapse, such as students wanting to keep certain information private from instructors [101]. By incorporating these features, social media platforms can help users navigate context collapse more effectively, and support privacy needs across a broader spectrum of scenarios and demographics.

9. Conclusion

Our interviews with Pakistani immigrants highlight the challenges that first-generation immigrants face navigating new technologies, coping with communication barriers and discrimination, and struggling to balance their new and old identities. Some of these challenges have persisted for years and are not at their core technological problems—for example, Americans have a long way to go to root out anti-Islamic prejudice. Still, left unchecked, technology can deepen these problems immigrants already face. However, under the right conditions, technology can also protect the privacy and security of immigrants.

As such, we conclude with a call for participation to help immigrants overcome the challenges they face and participate safely online. To this end, we believe that the security and privacy community should develop resources for immigrants that help them to be more aware of and better adapt to new security and privacy practices when transitioning to a new country. Likewise, developers could think carefully about cultural and religious contexts when they design products. For example, they could work to allow immigrants to have better tools for segmenting what content they share with whom. In this effort, it would be useful to work with second-generation immigrants who often know how to best reach their parents.

Acknowledgements

We are deeply grateful to our shepherd and anonymous reviewers for their efforts to help improve this work. This work was partially supported by the National Science Foundation under Grant Nos. CNS-2226404. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] A. Budiman, "Key findings about U.S. immigrants, Pew Research Center."

[2] U. M. International Organization for Migration (IOM), "Interactive world migration report 2022."

[3] V. M. Esses, "Prejudice and discrimination toward immigrants," *Annual Review of Psychology*, vol. 72, pp. 503–531, 2021.

[4] T. Bartkoski, E. Lynch, C. Witt, and C. Rudolph, "A meta-analysis of hiring discrimination against muslims and arabs," *Personnel Assessment and Decisions*, vol. 4, no. 2, p. 1, 2018.

[5] T. Fairless, "Immigration backlashes spread around the world," Jul. 2023, the Wall Street Journal, Accessed: 2024-2-3.

[6] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub, "Keeping a low profile? technology, risk and privacy among undocumented immigrants," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018, pp. 1–15.

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

[8] M. Tran, C. W. Munyendo, H. S. Ramulu, R. G. Rodriguez, L. B. Schnell, C. Sula, L. Simko, and Y. Acar, "Security, privacy, and data-sharing trade-offs when moving to the united states: Insights from a qualitative study," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 4–4.

[9] A. Budiman, "Pakistanis in the U.S. fact sheet," Apr 2021. [Online]. Available: https://www.pewresearch.org/social-trends/fact-sheet/asian-americans-pakistanis-in-the-u-s/

[10] X. Tang, Y. Sun, B. Zhang, Z. Liu, R. LC, Z. Lu, and X. Tong, "" i never imagined grandma could do so well with technology" evolving roles of younger family members in older adults' technology learning and use," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–29, 2022.

[11] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons, "Weighing context and trade-offs: How suburban adults selected their online security posture," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 211–228.

[12] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 309–325.

[13] International Organization for Migration, "Glossary on migration," 2019.

[14] J. C. Evans, "Hijacking civil liberties: The usa patriot act of 2001," *Loy. U. Chi. LJ*, vol. 33, p. 933, 2001.

[15] D. M. Silva, "The othering of muslims: Discourses of radicalization in The New York Times, 1969–2014," in *Sociological Forum*, vol. 32. Wiley Online Library, 2017, pp. 138–161.

[16] B. Mohamed, "Views of muslims in the U.S., 20 years after 9/11, Pew Research Center."

[17] S. Alimahomed-Wilson, "When the fbi knocks: Racialized state surveillance of muslims," *Critical Sociology*, vol. 45, no. 6, pp. 871–887, 2019.

[18] K. Engle, "Constructing good aliens and good citizens: Legitimizing the war on terror (ism)," *U. Colo. L. Rev.*, vol. 75, p. 59, 2004.

[19] S. Kamali, "Informants, provocateurs, and entrapment: Examining the histories of the fbi's patcon and the nypd's muslim surveillance program," *Surveillance & Society*, vol. 15, no. 1, pp. 68–78, 2017.

[20] T. Shams, "Visibility as resistance by muslim americans in a surveillance and security atmosphere," *Sociological Forum*, vol. 33, no. 1, pp. 73–94, 2018.

[21] P. M. Casey, "Stigmatized identities: Too muslim to be american, too american to be muslim," *Symbolic Interaction*, vol. 41, no. 1, pp. 100–119, 2018.

[22] T. Afnan, Y. Zou, M. Mustafa, M. Naseem, and F. Schaub, "Aunties, strangers, and the {FBI}: Online privacy concerns and experiences of {Muslim-American} women," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 387–406.

[23] S. Mare, A. Vashistha, and R. J. Anderson, "Security and privacy design considerations for low-literate users in developing regions," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*.

[24] S. Naveed, H. Naveed, M. Javed, and M. Mustafa, ""ask this from the person who has private stuff": Privacy perceptions, behaviours and beliefs beyond weird," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–17.

[25] S. Ibtasam, L. Razaq, M. Ayub, J. R. Webster, S. I. Ahmed, and R. Anderson, ""my cousin bought the phone for me. i never go to mobile shops.": The role of family in women's technological inclusion in islamic culture," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, nov 2019.

[26] A. Ashraf, C. J. König, M. Javed, M. Mustafa *et al.*, ""stalking is immoral but not illegal": Understanding security, cyber crimes and threats in Pakistan," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 37–56.

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

[28] F. Herbert, S. Becker, A. Buckmann, M. Kowalewski, J. Hielscher, Y. Acar, M. Dürmuth, Y. Zou, and M. A. Sasse, "Digital security—a question of perspective. a large-scale telephone survey with four at-risk user groups," in *2024 IEEE Symposium on Security and Privacy (SP)*.

[29] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "{"My} data just goes {Everywhere:"} user mental models of the internet and implications for privacy and security," in *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 2015, pp. 39–52.

[30] Y. Yao, D. Lo Re, and Y. Wang, "Folk models of online behavioral advertising," in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2017, pp. 1957–1969.

[31] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall, ""when i am on wi-fi, i am fearless" privacy concerns & practices in everyday wi-fi use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009, pp. 1993–2002.

[32] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, 2010, pp. 1–16.

[33] S. Altay and A. Acerbi, "People believe misinformation is a threat because they assume others are gullible," *New media & society*, p. 14614448231153379, 2023.

[34] M. Tabassum, T. Kosinski, and H. R. Lipford, "" i don't own the data": End user perceptions of smart home device data practices and risks," in *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, 2019, pp. 435–450.

[35] C. J. Dommeyer and B. L. Gross, "What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies," *Journal of Interactive Marketing*, vol. 17, no. 2, pp. 34–51, 2003.

[36] S. Oesch, S. Ruoti, J. Simmons, and A. Gautam, ""it basically started using me:" an observational study of password manager usage," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pp. 1–23.

[37] K. Luijkx, S. Peek, and E. Wouters, ""grandma, you should do it—it's cool" older adults and the role of family members in their acceptance of technology," *International Journal of Environmental Research and Public Health*, vol. 12, no. 12, pp. 15 470–15 485, 2015.

[38] T. Mendel and E. Toch, "My mom was getting this popup: Understanding motivations and processes in helping older relatives with mobile security and privacy," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 4, pp. 1–20, 2019.

[39] J. D. Portz, C. Fruhauf, S. Bull, R. S. Boxer, D. B. Bekelman, A. Casillas, K. Gleason, and E. A. Bayliss, ""call a teenager… that's what i do!"-grandchildren help older adults use new technologies: Qualitative study," *JMIR aging*, vol. 2, no. 1, p. e13713, 2019.

[40] C. Pang, Z. Collin Wang, J. McGrenere, R. Leung, J. Dai, and K. Moffatt, "Technology adoption and learning preferences for older adults: evolving perceptions, ongoing challenges, and emerging design opportunities," in *Proceedings of the 2021 CHI conference on human factors in computing systems*, 2021, pp. 1–13.

[41] F. J. Gutierrez and S. F. Ochoa, "Mom, i do have a family! attitudes, agreements, and expectations on the interaction with chilean older adults," in *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, 2016, pp. 1402–1411.

[42] T. Mendel, D. Gao, D. Lo, and E. Toch, "An exploratory study of social support systems to help older adults in managing mobile safety," in *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*, 2021, pp. 1–13.

[43] C. B. Fausset, L. Harley, S. Farmer, and B. Fain, "Older adults' perceptions and use of technology: A novel approach," in *Universal Access in Human-Computer Interaction. User and Context Diversity: 7th International Conference, UAHCI 2013,*.

[44] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, "Privacy and security threat models and mitigation strategies of older adults," in *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, 2019, pp. 21–40.

[45] S. Murthy, K. S. Bhat, S. Das, and N. Kumar, "Individually vulnerable, collectively safe: The security and privacy practices of households with older adults," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW1, pp. 1–24, 2021.

[46] N. Kanan, L. Arokiasamy, and M. R. bin Ismail, "A study on parenting styles and parental attachment in overcoming internet addiction among children," in *SHS Web of Conferences*, vol. 56. EDP Sciences, 2018, p. 02002.

[47] J. Xu, L.-x. Shen, C.-h. Yan, H. Hu, F. Yang, L. Wang, S. R. Kotha, F. Ouyang, L.-n. Zhang, X.-p. Liao *et al.*, "Parent-adolescent interaction and risk of adolescent internet addiction: a population-based study in shanghai," *BMC psychiatry*, vol. 14, no. 1, pp. 1–11, 2014.

[48] L. T. Lam, "The roles of parent-and-child mental health and parental internet addiction in adolescent internet addiction: Does a parent-and-child gender match matter?" *Frontiers in public health*, vol. 8, p. 142, 2020.

[49] W. Wang, D. Li, X. Li, Y. Wang, W. Sun, L. Zhao, and L. Qiu, "Parent-adolescent relationship and adolescent internet addiction: A moderated mediation model," *Addictive behaviors*, vol. 84, pp. 171–177, 2018.

[50] N. Alqahtani, S. Furnell, S. Atkinson, and I. Stengel, "Internet risks for children: Parents' perceptions and attitudes: An investigative study of the saudi context," in *2017 Internet Technologies and Applications (ITA)*. IEEE, 2017, pp. 98–103.

[51] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt, "Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–26, 2021.

[52] V. Steeves and O. Jones, "Surveillance, children and childhood," *Surveillance & Society*, vol. 7, no. 3/4, pp. 187–191, 2010.

[53] Y. Hashish, A. Bunt, and J. E. Young, "Involving children in content control: a collaborative and education-oriented content filtering approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 1797–1806.

[54] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and P. J. Wisniewski, "A matter of control or safety? examining parental use of technical monitoring apps on teens' mobile devices," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–14.

[55] S. Livingstone, L. Kirwil, C. Ponte, and E. Staksrud, "In their own words: What bothers children online?" *European Journal of Communication*, vol. 29, no. 3, pp. 271–288, 2014.

[56] E. Staksrud and S. Livingstone, "Children and online risk: Powerless victims or resourceful participants?" *Information, Communication & Society*, vol. 12, no. 3, pp. 364–387, 2009.

[57] N. Ahmad, A. Arifin, U. Asma'Mokhtar, Z. Hood, S. Tiun, and D. I. Jambari, "Parental awareness on cyber threats using social media," *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 35, no. 2, pp. 485–498, 2019.

[58] K. G. E. Elgharnah and F. Ozdamli, "Determining parents' level of awareness about safe internet use." *World Journal on Educational Technology: Current Issues*, vol. 12, no. 4, pp. 290–300, 2020.

[59] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur, "Parents' and teens' perspectives on privacy in a technology-filled world," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*.

[60] A. Czeskis, I. Dermendjieva, H. Yapit, A. Borning, B. Friedman, B. Gill, and T. Kohno, "Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety," in *Proceedings of the sixth symposium on usable privacy and security*, 2010, pp. 1–15.

[61] T. Leaver, "Intimate surveillance: Normalizing parental monitoring and mediation of infants online," *Social media+ society*, vol. 3, no. 2, p. 2056305117707192, 2017.

[62] A. Bryman, *Social research methods*. Oxford university press, 2016.

[63] S. Sultana, F. Guimbretière, P. Sengers, and N. Dell, "Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[64] S. Sultana and S. R. Fussell, "Dissemination, situated fact-checking, and social effects of misinformation among rural bangladeshi villagers during the covid-19 pandemic," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–34, 2021.

[65] O. of International Religious Freedom, "Pakistan - United States Department of State," *2022 Report on International Religious Freedom: Pakistan*, 2022.

[66] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[67] D. A. Gioia, K. G. Corley, and A. L. Hamilton, "Seeking qualitative rigor in inductive research: Notes on the gioia methodology," *Organizational research methods*, vol. 16, no. 1, pp. 15–31, 2013.

[68] W. Usman, J. Hu, M. Wilson, and D. Zappala, "Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 473–490.

[69] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[70] S. Zhang, Y. Feng, Y. Yao, L. F. Cranor, and N. Sadeh, "How usable are ios app privacy labels?" *UMBC Faculty Collection*, 2022.

[71] A. G. D. Holmes, "Researcher positionality–a consideration of its influence and place in qualitative research–a new researcher guide." *Shanlax International Journal of Education*, vol. 8, no. 4, pp. 1–10, 2020.

[72] M. Kovach, *Indigenous methodologies: Characteristics, conversations, and contexts*. University of Toronto press, 2021.

[73] I. Allison, "CAIR: New data shows the end of 2023 was a 'relentless' wave of bias, community resilience is 'impressive'."

[74] A. A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori, "Why they ignore english emails: The challenges of {Non-Native} speakers in identifying phishing emails," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021, pp. 319–338.

[75] D. Boyd, "Faceted id/entity: Managing representation in a digital world," *Unpublished Master's Thesis. Cambridge, MA: MIT*, 2002.

[76] M. Farrell, "Davis polk rescinded job offers for columbia and harvard students, but it may reverse itself - The New York Times," Oct 18 2023.

[77] A. McDonald, C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles, "" it's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 375–392.

[78] A. H. Qamar, "The concept of the 'evil'and the 'evil eye'in islam and islamic faith-healing traditions," *Journal of Islamic Thought and Civilization*, vol. 3, no. 2, pp. 44–53, 2013.

[79] T. Ishihara, M. Kobayashi, H. Takagi, and C. Asakawa, "How unfamiliar words in smartphone manuals affect senior citizens," in *Universal Access in Human-Computer Interaction. Applications and Services for Quality of Life: 7th International Conference, UAHCI 2013*, pp. 636–642.

[80] Q. Ma, A. H. Chan, and P.-L. Teh, "Insights into older adults' technology acceptance through meta-analysis," *International Journal of Human–Computer Interaction*, vol. 37, no. 11, pp. 1049–1062, 2021.

[81] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. S. Gaytán-Lugo, T. Matthews, S. Consolvo, and E. Churchill, "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 127–142.

[82] C. Women, "The mobile gender gap report 2019," *GSMA, London Retrieved from https://www. gsmaintelligence. com/research*, 2019.

[83] N. Rangaswamy and N. Sambasivan, "Cutting chai, jugaad, and here pheri: towards ubicomp for a global community," *Personal and Ubiquitous Computing*, vol. 15, pp. 553–564, 2011.

[84] P. Samermit, A. Turner, P. G. Kelley, T. Matthews, V. Wu, S. Consolvo, and K. Thomas, "Millions of people are watching you: Understanding the digital-safety needs and practices of creators," in *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 5629–5645.

[85] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 319–338.

[86] M. Fagan, Y. Albayram, M. M. H. Khan, and R. Buck, "An investigation into users' considerations towards using password managers," *Human-centric Computing and Information Sciences*, vol. 7, no. 1, pp. 1–20, 2017.

[87] P. Slovic, "Perception of risk," *Science*, vol. 236, no. 4799, p. 280–285, Apr. 1987. [Online]. Available: http://dx.doi.org/10.1126/science.3563507

[88] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," *The journal of psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[89] N. Abokhodair and S. Vieweg, "Privacy & social media in the context of the arab gulf," in *Proceedings of the 2016 ACM conference on designing interactive systems*, 2016, pp. 672–683.

[90] H. Rabaan, A. L. Young, and L. Dombrowski, "Daughters of men: Saudi women's sociotechnical agency practices in addressing domestic abuse," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW3, pp. 1–31, 2021.

[91] S. Ibtasam, "For god's sake! considering religious beliefs in hci research: A case of islamic hci," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–8.

[92] D. Oyserman, H. M. Coon, and M. Kemmelmeier, "Rethinking individualism and collectivism: evaluation of theoretical assumptions and meta-analyses." *Psychological bulletin*, vol. 128, no. 1, p. 3, 2002.

[93] H. J. Zhan, Z. Feng, Z. Chen, and X. Feng, "The role of the family in institutional long-term care: cultural management of filial piety in china," *International Journal of Social Welfare*, vol. 20, pp. S121–S134, 2011.

[94] S. Vieweg and A. Hodges, "Surveillance & modesty on social media: How qataris navigate modernity and maintain tradition," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2016, pp. 527–538.

[95] G. Harkness, "Out of bounds: Cultural barriers to female sports participation in qatar," in *Sport in the Middle East*. Routledge, 2017, pp. 64–84.

[96] A. J. Lim, C. Y. H. Lau, and C.-Y. Cheng, "Applying the dual filial piety model in the united states: A comparison of filial piety between asian americans and caucasian americans," *Frontiers in Psychology*, vol. 12, p. 786609, 2022.

[97] A. L. Freeberg and C. H. Stein, "Felt obligation towards parents in mexican-american and anglo-american young adults," *Journal of Social and Personal Relationships*, vol. 13, no. 3, pp. 457–471, 1996.

[98] J. W. DeCew, *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press, 1997.

[99] S. D. Farnham and E. F. Churchill, "Faceted identity, faceted lives: social and technical issues with being yourself online," in *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, 2011, pp. 359–368.

[100] M. Sleeper, R. Balebako, S. Das, A. L. McConahy, J. Wiese, and L. F. Cranor, "The post that wasn't: exploring self-censorship on facebook," in *Proceedings of the 2013 conference on Computer supported cooperative work*, 2013, pp. 793–802.

[101] V. P. Dennen and K. J. Burner, "Identity, context collapse, and facebook use in higher education: Putting presence and privacy at odds," in *Social Presence and Identity in Online Learning*. Routledge, 2020, pp. 37–56.

Appendix A. Study Materials

A.1. Eligibility Criteria

*You are at least 18 years old and fall into **one** of the following groups:*

1) *You emigrated from Pakistan to the US with a child who was 13 years old or under.*
2) *You emigrated from Pakistan to the US and then had a child in the US who is now at least 13 years old.*
3) *You emigrated from Pakistan to the US with your parents when you were 13 years old or under.*
4) *Your parents emigrated from Pakistan to the US and you were born in the US.*

A.2. Interview Protocol

"We are interested in how immigrants use technology. This is important to us because a lot of the time, technology is not easy to use, and this is the fault of the technology, not the people using it. So, we want to hear about your experience with technology, so that we can improve technology for others. This means that if there is anything that is hard for you to do or any technology that is hard to use, we really want to hear about it, so we can try to fix it."

- Do you have any questions before we start?
- How frequently do you use the following devices? (Daily, Once or twice a week, Once or twice a month, Rarely, Never, I don't own this type of device)
  - Desktop or laptop
  - Smartphone
  - Tablet
  - Smartwatch
  - Smart speaker (like Alexa, Google Nest, etc.)
- (For each device) What do you use [the device] for?
  - Social media
  - Online/mobile banking
  - Online shopping
  - Watching videos
  - Playing games
- Which social media apps/websites do you have an account on?
  - How frequently do you use them?
- (1st Generation) Many people use their device to communicate with people back home. Does your family use any apps to do this?
  - How did you choose the app?
  - Any stories about using or setting up the app?
- Is there anything different about your experience using technology in the US as compared to Pakistan?
  - What was the biggest change? Was it positive or negative?
  - What was the hardest change?
  - Is there anything you wish people in the US did more like people in Pakistan?

- If you give one or two pieces of advice to a new immigrant regarding technology in the US, what would that be? Why do you suggest this?
  - Are there any apps or technologies that you find to be especially useful?

- (1st Generation only)
  - Do you rely on your children to help you use the internet? How so?
    - Can you think of a specific time when they helped you?
    - Have there ever been any disagreements during this process?
    - Have your children relied on you to use the internet? What did that look like?
    - Did you feel that you had to do more than your non-immigrant friends to educate your children?
- (2nd Generation only)
  - Has there been a time where you needed to help your parents with technology?
    - What was it? How did it go? Were they receptive?
    - Have there ever been any disagreements during this process?
    - Have your children relied on you to use the internet? What did that look like?
  - Have your parents helped you use technology before? What did that look like?
- What do you do to be safe on the internet?
- What security and privacy advice would you give to a new immigrant?
  - Why do you suggest this?
- (1st Generation only)
  - Do you think you and your children have similar internet safety habits?
    - Where did you/they learn your internet safety habits?
  - What types of security and privacy advice do you give to your children?
    - Which of these is the most important?
    - Do you feel your children are receptive to your advice? Why or why not?
  - What types of security and privacy advice do your children give to you?
    - Which of these is the most important?
    - How receptive are you to their advice? Why?
- (1st Generation only)
  - Do you think you and your parents have similar internet safety habits?
  - Where did you/they learn your internet safety habits?
  - What types of security and privacy advice do you give to your parents?
    - Which of these is the most important?
    - Do you feel your parents are receptive to your advice? Why or why not?
  - What types of security and privacy advice do your parents give to you?
    - Which of these is the most important?
    - How receptive are you to their advice? Why?
  - Are there any interesting stories you have about security and privacy? Any incidents that you can remember?
- Who or what do you think are the biggest threats when it comes to being safe online?
  - How likely are these threats to occur?
  - Has it happened to you before?
  - What do you do to address these threats?
  - Do you face any difficulties in doing so? (Barriers)
  - How effective are these mitigations?
  - What would be the consequences if those [threats] happened to you?
- Do you share your devices with other people?
  - In what situations do you share? Why?
  - How does this sharing impact your use of the device?
  - If you could choose not to share would you? Why?
- Is there any information you don't like putting online?
  - How do you store this information?
  - Are you worried that someone might steal the information you put online?
    - Has this ever happened to you?
- Who do you think knows more about being safe online, you or your child/parent?
- Do you post about politics on your social media?
  - Why or why not?
- Do you post about religion on your social media?
  - Why or why not?
- What are your thoughts on passwords?
  - Do you think they protect you enough? Why or why not?
  - What tips do you have for keeping your password safe?
  - How do you create passwords that you can remember?
  - How do you remember your passwords and remember which accounts go with which passwords?
    - Do you use a password manager? Why or why not?
  - Do you share any of your passwords with anyone?
    - How do you go about sharing passwords?
    - What do you do if you don't want to share that password anymore?
  - Do you use an authenticator app or an HSK? Why or why not? (2FA question)
  - Have you ever used a VPN? Why or why not?
  - Some websites have you answer security questions if you forgot your password. Have you ever experienced this?
    - Did you find these questions easy to remember? Why or why not?

Appendix B.
Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

B.1. Summary

This work explores the security and privacy perceptions, practices, and challenges of Pakistani immigrants in the US, and how family dynamics affect these through 25 semi-structured interviews with Pakistani immigrants. This paper identifies several challenges such as language barriers, discrimination, online privacy concerns, and adapting to technology. This paper identifies key generational differences like first generation immigrants have increased risks of discrimination, surveillance, and isolation, while second generation immigrants do not. First and second generation immigrants works together in learning how to use technology and managing perceived threats.

B.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Provides a Valuable Step Forward in an Established Field

B.3. Reasons for Acceptance

1) Methods are well-thought out with the use of semi-structured interviews and qualitative analysis.
2) Paper is very well-written and easy to read. The narrative of the paper flows well and the takeaways are clear.
3) Recommendation are rooted in the result with clear takeaways stemming from what was learned through the interviews. The recommendations of this work will likely benefit other immigrant populations as well.
4) Relevant and timely issue as there has been little research exploring the security and privacy concerns of immigrants and immigrant-family dynamics. This research provides a valuable foundation for future work.