

USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Sharing Digital Devices is Normal and Cultural: Privacy and Security Challenges in Collectivist Immigrant Households

S. Shanza, *University of Waterloo;* Ameemah Humayun, *Lahore University of Management Sciences;* Urs Hengartner and Leah Zhang-Kennedy, *University of Waterloo*

https://www.usenix.org/conference/soups2026/presentation/shanza

This paper is included in the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security is sponsored by USENIX.

Sharing Digital Devices is Normal and Cultural: Privacy and Security Challenges in Collectivist Immigrant Households

S. Shanza
University of Waterloo
sshanza@uwaterloo.ca

Ameemah Humayun
Lahore University of Management Sciences
26100175@lums.edu.pk

Urs Hengartner
University of Waterloo
urs.hengartner@uwaterloo.ca

Leah Zhang-Kennedy
University of Waterloo
lzhangkennedy@uwaterloo.ca

Abstract

In collectivist households, sharing digital devices is both a cultural norm and often necessary. After migration to more individualistic cultures such as Canada, these sharing practices persist but become entangled with new cultural norms and highly digitized systems. We report findings from a qualitative study of 18 nuclear families (19 parents, 22 children) mainly from South-Asia examining how migration and sociocultural factors shape security and privacy risks in multi-user households and how current devices support or hinder safe sharing. Shared-device use exposed families to data breaches, reputational harms, cultural and religious boundary violations, and intergenerational tensions. At the same time, coping strategies were often fragile or abandoned when they threatened family harmony. Our findings reveal a structural mismatch between single-user device assumptions and collectivist immigrants' household realities. Designing for shared-device contexts is therefore essential for building more inclusive digital infrastructures that support multicultural families and others who rely on device sharing.

1 INTRODUCTION

Nearly one in four Canadians is an immigrant, with a significant proportion associated with "collectivist" regions [89]. Hofstede [45] defines collectivist cultures as those in which individuals see themselves primarily as members of tightly knit social groups, prioritizing loyalty and relational obligations over individual autonomy. These orientations manifest in practices like multi-generational living, pooled resources, and collective decision-making [82, 94]. In these communities, device sharing is highly prevalent [5, 6]. Device sharing can also occur in non-collectivist households where devices are lent, borrowed, or otherwise shared in situational and impromptu contexts [48, 53, 60, 63]. However, it differs significantly from collectivist households by the associated frequency and contextual factors [6, 55], where devices are treated as communal assets, with access negotiated based on age, gender, purpose, and trust rather than individual ownership [6, 71]. Yet, contemporary devices largely assume a single user, with authentication and access controls often designed for one signed-in individual [16, 59, 101]. Although some offer separate profiles or guest modes [13, 70], these mechanisms rarely accommodate the social realities of collectivist households [5, 6, 71, 83].

These dynamics are further complicated by migration; prior literature describes how migrants remain embedded in practices shaped by their countries of origin while navigating the host society, causing a blend of value systems [62, 98]. Simultaneously, life in WEIRD (Western, Educated, Industrialized, Rich, and Democratic) contexts is increasingly mediated through digitized systems, limiting families' ability to opt out [34, 98, 100]. Immigrant families must rapidly adapt to new digital infrastructure while upholding home country values. This tension is heightened by discrimination, weak support networks, and remains largely ignored [18, 33, 36, 85].

Furthermore, when families share devices, children face compounded privacy risks: their browsing histories, messages, and social media activity become visible to other household members, while their own risk-taking behaviors online expose them to cyberbullying and fraud [15, 61, 104]. These risks also put others sharing devices with them at risk, with every consequence becoming a household problem. Parents attempt to mitigate risks through monitoring and guidance [11, 39, 41, 99], yet such measures often strain relationships [9, 29, 38, 103]. These dynamics are intensified for immigrants, who often have limited social and technical support networks in the new digital landscape [93, 98]. Despite these factors, there is limited understanding of how parent-child dynamics shape privacy and security in immigrant families navigating shared-device environments [98].

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

We conducted 41 semi-structured one-on-one interviews with parents and their children from 18 voluntary migrant[1] families (predominantly from South Asia) in Canada to answer the following research questions:

RQ1. *How do cultural values, religious beliefs and intergenerational dynamics shape how and why immigrant families share digital devices post migration?*

RQ2. *What privacy, security, social and moral risks arise in shared-device households, and how do families manage and negotiate these challenges?*

RQ3. *How usable and effective are current devices for shared use, and how can they better support safe sharing?*

Our findings highlight a fundamental mismatch between individual-centric devices and the lived realities of collectivist immigrant households. We find that migration-related transitions compound device sharing challenges in collectivist households, and that Security and Privacy (S&P) risks on shared devices can lead to reputational harm, cultural and religious boundary violations, and intergenerational tensions. We explore how sharing devices erodes intra-family privacy, how dependents use concealment to navigate parental surveillance, and how parents struggle to balance cultural preservation with host-country norms. We find that families rely on ad hoc, post hoc, and behavioral strategies to manage these risks, largely because usable system-level support for device sharing is unavailable and because families face complex setups with limited technical knowledge. This includes keeping devices in a "morally clean" state, install-delete app cycles, or using decoy and stealth tools. However, these coping strategies are often insufficient and strain family bonds. Rather than value-neutral tools, shared devices function as culturally governed infrastructures where visibility and control reflect family authority and moral expectations. We analyze sharing challenges and participant-requested features that reveal deeper needs that are poorly supported by single-user device designs in collectivist households. We therefore argue for devices that account for diverse sociocultural contexts and treat device sharing as an important design consideration.

2 RELATED WORK

We organize prior work into two strands: (1) S&P challenges faced by migrants, and (2) device sharing in collectivist cultures and family dynamics that affect them.

2.1 Migrants and S&P Challenges

Migrants rely heavily on digital technologies to meet everyday security, privacy, and transnational needs [27]. Migration introduces a new digital landscape that is particularly difficult to navigate for individuals from developing countries, due to risks that disproportionately affect marginalized groups, like language barriers and heightened exposure to scams, surveillance, and fraud, further compounded by discrimination and isolation [18, 33, 36, 51, 52, 95]. Many experience "privacy turbulence" due to uncertainties in the host country [91]. Prior work documents the digital vulnerabilities of marginalized migrants, including Muslim-American women and migrant domestic workers, who face harassment and surveillance [88]. For example, norms around modesty, gendered visibility, and moral accountability continue to shape digital practices in Muslim diasporic contexts [50, 69]. Similarly, expectations of modesty are common to other religious contexts as well, including Hindu and Christian [14, 30], and these values are extended to digital spaces, posing reputational harm and several other consequences [4].

For immigrants navigating shared-device and collectivist digital environments, these harms are often amplified, as individual privacy or security failures can rapidly become household-level crises. Despite this, limited attention has been paid to S&P issues among immigrants [85], to the concerns, attitudes, and behaviors of minoritized ethnic communities [80], and to how device sharing is shaped by these transnational cultural values. Existing work focuses mainly on U.S.-based populations such as international students, undocumented immigrants, refugees, and migrant domestic workers [40, 88, 93, 97, 102], while large-scale representative work on migrants' security experiences specifically remains scarce [44]. Studies on Asian immigrants also tend to center on adults, leaving young children understudied [93, 98].

To address these gaps, we examine how migration-related and sociocultural factors shape immigrant families' S&P challenges, particularly for young dependents in shared-device contexts. By including parents, children, and young adult dependents from the same household, we capture within-family perspectives to show how S&P challenges unfold across generations and age groups.

2.2 Device-Sharing in Collectivist Cultures

Many communities frequently share technology labeled as "personal" conventionally [6,63], challenging Western notions of "personal computing" [17, 96]. Matthews et al. [63] classified these practices into borrowing, mutual use, setup, helping, broadcasting, and accidental access. This includes both devices [24, 54, 55, 57, 90] and accounts [31, 56, 66, 73, 87]. Device sharing is not limited to, but is more prevalent in collectivist and developing regions [6, 54, 67, 90]. Yet authentication and access controls remain largely designed for individual use [16, 96]. A U.S. study shows that when sharing devices, users selectively grant access and adjust authentication [78], and have strong expectations for individual control even for devices that are expectedly shared, such as smart speakers [1, 64]. In contrast, prior work shows that in collectivist settings, even personal devices such as phones are frequently shared [5]. Privacy is frequently viewed as secondary to collectivist needs [83], and device sharing is justi-

[1] Voluntary migrants refers to people who migrated primarily by choice (e.g., for work, education, or family reasons) rather than through forced displacement categories (e.g., as refugees or asylum seekers).

fied through narratives of care and tradition rather than surveillance [8] though such practices can also generate tension and moral judgment within hierarchical family structures [9]. Further, enforcing strict individual privacy controls can strain relationships with family and friends [5, 28].

Widespread device sharing combined with the sensitive nature of data on devices heightens risks such as misuse, moral judgment, blackmail, account compromise, and data leakage [5, 6, 10, 50, 55, 76, 83]. Social, cultural, and economic conditions [25, 75, 84], as well as religion [2, 3], shape these practices and gender norms and further exacerbate them leading to unequal access to devices and constant surveillance of women [4, 49, 68]. Daughters often face stricter limits on mobility, social interactions, and online activity because families worry about modesty, safety, and reputational harm tied to family honor [49, 68]. Also, device-sharing prompts ad hoc protections [5]. Although attempts to separate shared and hidden accounts exist, such as a tiered privacy model [6], their effectiveness remains unclear.

Because children are central actors in shared-device ecosystems [77, 99], parental mediation practices have significant implications for privacy and security. Dialogue-based mediation is associated with more positive outcomes [26, 99], whereas restrictive monitoring can undermine children's technical and social digital skills [26, 61, 99]. Evidence from collectivist contexts highlights additional challenges, including risky teen behaviors and difficulties with parental mediation amid rising device access [81]. Lack of research in this area leaves immigrant families unsupported as these device sharing challenges migrate to host countries with them [77, 98].

To address these gaps, we interviewed parents and dependents to examine how sociocultural values shape device governance, and how families negotiate tensions between collectivist sharing norms and individual privacy needs. Our sample centers predominantly first-generation South Asian immigrant families in Canada, offering a situated window into these dynamics within a specific yet underrepresented community. Capturing both perspectives of the parent–child dyad within the same families reveals relational tensions that single-sided studies miss and current tools fail to support.

3 METHODOLOGY

Terminology: In this paper, "dependents" refers to children (9–12), teens (13–17), and young adults (18-25), reflecting their non-parental familial role. Young adult dependents were included because many in migrant families still live with parents, enabling insight into both current and past device sharing dynamics. We define digital "devices" as personal smart technologies conventionally used individually but shared in collectivist families as discussed in Section 2.2. This includes devices storing personal data and supporting activities such as communication, browsing, and financial transactions (e.g., smartphones, tablets, laptops, desktops), and excludes communal devices (e.g., IoT devices, smart TVs) as they carry different privacy expectations. Across interviews, participants mostly spoke about devices collectively rather than individually or by type.

3.1 Participant Recruitment

We recruited through university-affiliated and community-based channels, including collaborations with organizations serving newcomer communities, and in two cases, snowball sampling. The screening form (completed by a parent), collected information about the families' country of origin, duration in Canada, device sharing information, language compatibility, and dependents' age. We received 259 screening responses for eligibility verification. The relatively low participation rate in the main study was due to non-response to follow-up interview invitations and scheduling constraints. Participants were eligible if parents were first-generation immigrants and the family had lived in Canada for 6 months to 20 years. This range captured varying stages of settlement, where country-of-origin norms and adaptation to Canada remained salient; length of residence is also commonly used as a proxy for acculturation [65]. We did not include non-immigrant families because prior literature already establishes baseline device sharing practices in Western contexts [10, 53, 55, 60, 63]. Instead, we report participants' comparisons of pre- and post-migration experiences and perceived differences from non-immigrant families. Eligible families had to share at least one device, as defined in this study, and include at least one parent and one dependent. Additional household members could participate voluntarily without additional compensation. Young adults were eligible as dependents if they lived with and shared devices with their parents. We targeted families originating from collectivist cultures, analyzed based on Hofstede's scale [45, 46]. Our final sample predominantly (13 of 18 families) reflects nuclear and first-generation South Asian immigrant families, with the majority identifying as religious. We focused on nuclear family households to reduce structural variability, since non-nuclear households may introduce additional layers of authority, device ownership, and intergenerational negotiation. This decision allowed for more comparable cross-household analysis.

3.2 Interview Protocol

The first author conducted all interviews, with each session lasting approximately 90 minutes and mostly in-person, with about 20% being online due to participants' preference or distance. To reduce priming, we used partial disclosure during recruitment and consent, describing the study as examining family technology use and shared-device practices without its focus on S&P. We developed two semi-structured interview protocols: one for parents and one for dependents with few variations adapted and simplified language for younger

children. Both protocols covered the same topics relating to device sharing (ownership and sharing practices, household rules, conflicts, and power dynamics, S&P concerns, cultural and religious influences on digital norms, and migration-related changes). The parent protocol also emphasized household governance, mediation strategies, online safety concerns, and navigating cultural values post-migration. The dependent protocol focused on monitoring experiences, privacy negotiation, comfort sharing, visibility management, and perceptions of parental rules. Both protocols included questions about past S&P incidents, coping strategies, and desired design features. Protocols were iteratively refined through six pilot interviews. An overview of both protocols is included in Appendix C.

3.3 Data Analysis

Interviews were audio-recorded and transcribed using *Trint*[2], a GDPR-compliant service selected for its multilingual support and security protections. Transcripts were manually reviewed for accuracy and analyzed in *Atlas.ti*[3] using reflexive thematic analysis [23]. This approach recognizes researchers' active, reflexive role in generating knowledge, with codes reflecting their interpretations of meanings and patterns in the data (see Section 3.4). Interviews were conducted primarily in English, with some conducted partially or fully in Hindi/Urdu based on participant preference. The interviewer is fluent in all three languages, which supported accurate comprehension of regional dialects without relying on a formal translation protocol. The interview guide is provided in Appendix C.

Recruitment was guided by the principle of thematic saturation, defined as the point at which no new themes emerged. Interviews were coded iteratively and in parallel with recruitment. This allowed emerging themes to be identified and refined. After approximately 14 families (33 participants) had been interviewed, few new themes emerged, suggesting we were approaching saturation. Recruitment and coding continued with four additional families. No new themes emerged in the final three interviews, suggesting thematic saturation.

Coding was conducted at the family level, treating each family as a unit of analysis. Two authors independently coded the first six interviews using inductive open-coding [92], then met to resolve conflicts in their codes through discussion to develop the first codebook. The first author refined the codebook by applying it to four additional interviews to ensure completeness. Approximately half of the remaining interviews were double-coded to support analytic consistency. After each coding round, coders met to compare interpretations and resolve discrepancies through reflexive discussion, and iteratively refine the codebook [47]. A sample of the final codebook is provided in Table 3 in Appendix D.

[2] https://trint.com/
[3] https://atlasti.com/

3.4 Positionality Statement

The research team brings diverse cultural and migration backgrounds that informed both data collection and interpretation. The first author is a recent first-generation immigrant from Pakistan currently living in Canada. The second author resides in Pakistan. The third and fourth authors are Canadian citizens; the third is a first-generation immigrant of European descent, and the fourth is a Chinese-Canadian second-generation immigrant. The first and second authors served as primary coders and brought lived experience with shared-device practices and collectivist cultural contexts, informing culturally grounded interpretations. To mitigate bias, interpretations were discussed with the entire research team, allowing insider perspectives to be complemented by analytic distance.

3.5 Ethical Considerations

Our Study received approval from our University Research Ethics Board. We followed established ethical guidelines thoroughly to protect participant safety and confidentiality [19]. Details are provided in Appendix A.

4 Limitations

Although our sample included immigrants from various countries of origin and religious backgrounds, it may not represent the full range of collectivist immigrant family experiences. Recruitment from mid- to large Canadian cities may also under-represent families who are geographically remote or less digitally connected (Section 6.2). While collectivist household dynamics serve as the broader conceptual lens for this work, the families in this study are predominantly first-generation South-Asian immigrants. Findings should be understood as reflective of this community.

In most households, only one parent enrolled and participated. As a result, our findings reflect the participating parent's account and may not capture differences between partners' views on device sharing and privacy.

The interviewer's language abilities and our recruitment channels may have introduced sampling bias, potentially excluding households whose primary language fell outside this range. As with qualitative work more broadly, our findings also rely on self-reported accounts, which may have be influenced by recall limitations or social desirability.

5 FINDINGS

We present our findings in three sections: (RQ1) device sharing practices in immigrant families and the influence of sociocultural factors; (RQ2) the S&P challenges that arise during sharing and families' mitigation strategies; and (RQ3) participants' perceptions of how effectively current devices support sharing practices and recommendations for making them safer. To help readers gauge how widely themes appeared, we report relative prevalence by participant group using ranges

Table 1: Summary of self-reported participant demographics across 19 parents and 22 children from 18 families.

Participant Role		**Family Religion**		**Immigration Stream**		**Country of Origin**	
Father (17.1%)	7	Muslim	11	Express Entry	10	Pakistan	5
Mother (29.3%)	12	Christian	4	Skilled Worker	2	India	4
Son (19.5%)	8	Sikh	1	Family Sponsorship	3	Iran	2
Daughter (34.1%)	14	Hindu	1	Student/Work/Other	3	Bangladesh	2
		Atheist	1			Ukraine, Zimbabwe, Eritrea	1 each
						Afghanistan, Palestine	1 each
Parent Occupation		**Parent Education**		**Parent Age**		**Dependent Age**	
Engineering/Technology	8	College Diploma	1	30–40 years	9	9–12 years	10
Business	5	Bachelor's	7	41–49 years	6	13–17 years	6
Education/Health/Other	6	Graduate Degree	11	50–59 years	4	18+ years	6
Household Size		**Years in Canada**		**Household Income (CAD)**		**Shared Devices**	
3 people	4	0.5–3 years	5	<50K	5	Smartphones	19
4 people	8	4–9 years	6	50–99K	5	Laptops	19
5+ people	6	10+ years	7	100K+	8	Tablets	13

following prior work [32, 86, 106], as shown in Figure 1.

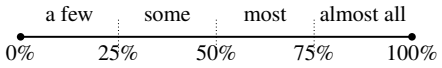


Figure 1: Terminology used to present relative frequency.

Participant Demographics: Table 1 presents a summary of participant demographics. All findings are situated within nuclear families comprising 2–3 participants each, typically one parent and one or two dependents (five families included three participants). The average number of people per family that shared devices was three.

Participant Notation: Participants are identified with a unique ID (1-41) prefixed by role: M (Mother), F (Father), S (Son), D (Daughter) (e.g., M3 denotes mother #3). To reduce the risk of identifying individuals within families, we did not link participants' familial relationships in the findings.

Device-Sharing in Practice: Before presenting our thematic findings, we briefly characterize device sharing across participating households. Sharing centered on personal devices, most commonly smartphones and laptops, with tablets also frequently shared (Table 1). Participants used shared devices for schoolwork, gaming, communication, entertainment, creative activities, photography, and social media. Sharing was shaped by convenience, parental monitoring, financial constraints, safety, coordination, bonding, and broader cultural expectations around collective access and responsibility. We distinguish shared *devices*, where multiple household members use the same hardware, from shared *accounts*, where members access a common login. In practice, these often overlapped, as participants described shared devices alongside shared accounts.

30% of dependents reported sharing devices daily and 35% weekly, while parents similarly reported frequent device sharing and mutual device use within households. Interviews revealed that sharing was often deeply embedded in everyday family routines and frequently extended beyond discrete sharing events. The findings that follow examine how these practices were shaped by migration, cultural expectations, and family dynamics (Section 5.1), how they differed from participants' experiences in their countries of origin; and the privacy and security challenges that emerged due to these factors (Section 5.2).

5.1 (RQ1) Sociocultural Dynamics of Sharing

> *Culturally we just tend to share things. We were taught that you should be able to share things with others, you know, just be cordial rather than "this is mine, it's only mine." (M18)*

This sentiment reflects how participants framed device sharing as a cultural norm rather than a technical choice. In this section, we examine how parents and dependents navigate the sociocultural impacts of migration on sharing norms, including shifting expectations, power dynamics, and how device sharing practices evolve post-migration.

5.1.1 Home Country to Host Country

Almost all parents wistfully contrasted device sharing norms before and after migration. In their home countries, most parents described limited need for personal devices due to closer supervision, denser social networks, and more structured routines, reducing both device provision and sharing. After migration, increased work and settlement demands reduced parental oversight while dependents had more unstructured time, easier device access, and fewer environmental restrictions. These shifts led to earlier device provision and increased reliance on device sharing as a compensatory monitoring strategy. Some parents described giving dependents devices at a young age, often reluctantly: *"If I was in [my country]... before going to college, I would never give them the phone... here I had to give it... it was very stressful... it was actually a fear"* (M16). Because early independent ownership was viewed as a loss of control and culture, most parents adopted device sharing to regain oversight of use and relied on devices as tools for cultural transmission (Section 5.1.2). Migration-related loss of family supervision further reinforced this shift, increasing

reliance on shared devices for coordination and monitoring.

Decisions about dependents' device ownership were shaped by maturity, peer norms, monitoring capacity, and migration-related concerns about sharing as a moral safeguard. Some parents delayed personal ownership until children demonstrated moral readiness: *"When I see that they are God fearing... then I will give it"* (M9). Others framed continued sharing as resisting *"becoming more Canadian"* (F1), positioning it as a compromise between maintaining cultural norms and avoiding conflict. Post-migration safety concerns, such as online bullying (M16), further reinforced sharing as protective. Across households, device sharing expanded post-migration to support monitoring, coordination, safety, bonding, and financial management, rather than the more limited or situational sharing described pre-migration.

5.1.2 Devices as Tools for Cultural Transmission

Most parents used shared-device control to regulate dependents' exposure to cultural, religious, and political content that was seen as conflicting with home-country values. A few restricted access to specific platforms or content categories, and some avoided providing independent devices altogether to retain oversight through device-sharing.

Shared access also supported cultural transmission, with some families embedding religious practice into device use: *"We have like Quran apps... we'd have to read Quran to even be able to use our phones... it's kinda like a reward"* (S37). Others monitored religious content due to fears of radicalization: *"... children go towards extremism; become a fundamentalist. I was very scared of that. I never encouraged them to watch any [XYZ] content"* (M16). Parents similarly scrutinized media such as games for perceived ideological conflict, sometimes framing certain content as anti-religious or "propaganda," a view some dependents themselves adopted: *"My son himself often tells me... he thinks that propaganda it's pushing"* (M16). Overall, shared devices functioned not only as safety tools but as mechanisms of cultural transmission and value enforcement after migration.

5.1.3 Migration-Driven Social Regulation

Most parents viewed risky behaviors as arising from online influence and imitation, which they felt were intensified after migration. To counter these risks, almost all families reported stricter monitoring and greater reliance on shared devices than they considered necessary in their home countries. In Canada, shared devices became a primary means of regulating dependents' exposure to online and peer influences perceived as conflicting with religious or moral values. For example, M9 choose to home school their children to *"shield them... [from] content that might conflict with our religion."* Within these contexts, sharing enabled continuous parental visibility and intervention, narrowing privacy boundaries.

Parents regulated dependents' social relationships through shared-device oversight, particularly for younger children, restricting contact with peers who they saw as enablers of risky online behavior. For example, one child uploaded private family videos to YouTube via a shared-device under peer influence, exposing personal details (M12). Romantic or cross-gender interactions were often prohibited across age groups, and dependents reported concealing such activity to avoid conflict. Across households within Muslim, Sikh, and Christian backgrounds, shared-device access functioned as a central mechanism for monitoring and constraining social ties and online self-presentation. Dependents said this regulation extended to siblings, who sometimes acted as informal informants: *"My brother told my mom that I have a boyfriend on Snapchat, which I don't"* (D26). Even where families adopted some host-country norms, shared-device oversight maintained limits on digital expression. One family allowed dating for an 18-year-old daughter but prohibited posting about it online, fearing judgment from the *"extended family"* (M16). Overall, sharing maintained home-country values while navigating new social norms, with stricter surveillance for children and greater flexibility for older dependents entering adulthood.

5.1.4 Social and Religious Screening of Devices

Cultural expectations and religion almost always shaped digital rules. Most parents described deliberate efforts to promote religious content through devices and to maintain moral and religious "hygiene," keeping shared devices free from material deemed inappropriate or corrupting. As F2 explained, *Both of these phones are completely Islami [religious] and there is nothing here that I cannot share with my kids... "* Most parents also avoided using certain apps (e.g., Facebook, TikTok) not for safety reasons but to maintain self-censorship. Almost all dependents (aged 9-17) recognized these expectations as well, avoiding content they considered "bad," that is, "religiously or culturally inappropriate." Device rules were thus framed as moral expectations: compliance signaled being a "good" child, while misuse was treated as moral failure rather than rule-breaking. Privacy and device access became conditional privileges tied to obedience, or academic performance, a view few dependents internalized, describing those with shared access as "well-behaved" and those who do not as "ill-mannered" or "not doing well at school" (S37). These moral expectations extended to young adult dependants and even parents' own online self-presentation. In a few families, requirements such as religious dress (e.g., hijab) in photos were enforced through shared-device control, including deleting non-compliant content.

A few others imposed broader restrictions on what could be shared publicly, reviewing children's activity through shared accounts or devices for content perceived as conflicting with cultural, religious, or privacy values: *"In cases of trending stuff like dances... There is a cultural aspect, religious aspect, or privacy aspect so we don't want [our daughter] to share publicly"* (F2). These rules were often driven by fears of reputational harm and community judgment, and concerns

were more salient for daughters: *"We feel the pressure from our community... we will get judgment... unsolicited advice" (F2).* Almost all dependents, regardless of their age, described concealment strategies such as hiding or deleting activity on shared devices to avoid moral or religious judgment.

5.1.5 Negotiating Culture in New Digital Contexts

Parents' upbringing and migration histories strongly shaped device governance. While some families softened digital rules over time, most parents continued to apply pre-migration norms that dependents saw as outdated or mismatched with Canadian expectations. One participant explained this as "unfair," as her father delayed her phone ownership based on his own childhood experience, forcing device sharing practices: *"Like obviously they weren't raised in bad neighborhoods but, I feel like [my country]'s obviously very different from Canada."* (D20). Thus, while host-country expectations favored earlier individual ownership, migration often preserved home-country sharing practices, producing intergenerational conflict over autonomy and device access. A few parents described deliberately shifting toward more flexible, "Canadian-style" device governance by rejecting aspects of their own upbringing. Reflecting on their childhood, M16 noted, *"The way we were raised, we were very submissive, and we used to feel very frustrated."* These shifts often produced less restrictive sharing and more trust-based autonomy than parents had initially envisioned. For most families, migration-related cultural change and growing parent-dependent divergence created uncertainty, leading them to negotiate sharing rather than rely on strict control: *"If we keep them under strict rules, they will go away from us... I saw it very clearly that it had a counter-productive effect... It was better to discuss and talk about it"* (M16). Thus, while home-country norms favored hierarchical, prolonged sharing and oversight, migration sometimes encouraged more flexibility.

Some parents expressed this resignation: *"Some of these things are impacted by the culture and the religion... but I try not to impose these things on them, and I try to be open-minded, but it's very difficult"* (M12), and *"What else can we do?"* A few practiced "strategic ignorance," avoiding scrutiny of dependents' activities on shared devices (M16), while others moderated reactions to maintain disclosure (M12). This was done by parents to preserve family harmony. However, a few parents expressed regret about relaxing rules after migration: *"I wish I weren't allowed her to download some app... When I was in my home country, I had a rule... you can have this app at 14 years old"* (M14). These tensions reflect that most migrant parents have difficulty balancing cultural values with host-country norms, which shape how risks are managed on shared devices, motivating a closer examination of the security and privacy landscape families navigate.

5.2 (RQ2) Shared-Device S&P Landscape

> *We all share everything... transparency is very important in our culture. (D28)*

Within shared-device use, transparency is a family value, but it makes personal boundaries difficult to maintain. Our findings show that challenges arise not only from technical vulnerabilities but also from sociocultural and religious boundary violations. Together, these factors shape the risks and coping strategies families develop on shared devices post-migration.

5.2.1 New Country, New Threats

A few participants reported heightened S&P concerns after migrating to Canada, consistent with prior work on collectivist groups' and immigrants' scam vulnerability [42,44,51,52,95]. In shared-device households, these threats often affected multiple family members rather than individuals alone. Incidents such as malware, hacking, password breaches, and harassment caused household-wide disruption when compromised accounts, contacts, or visible content affected others using the same device. Shared access and credentials also made unfamiliar Canadian threat environments, such as phishing calls, harder to navigate: *"Somebody called him and asked [my son] to give his passcode...for three or four days it stayed hacked"* (M16). Some scams exploited new commers' unfamiliarity with local systems, such as deportation threats leveraging fear and limited awareness: *"when we first came to Canada... they said we're going to deport you back... and we actually thought it was true... we were a bit scared"* (D28). Such incidents often prompted changes in sharing practices, including increased monitoring or restricted access.

5.2.2 One Device, Too Many Users

Almost all participants mentioned how shared devices created distinct S&P vulnerabilities, as digital traces (e.g., chats, usage history, purchases) could be seen, misinterpreted, used to make judgments, or sparked conflict among family members. Because device sharing was so common, some felt overwhelmed, confused, or frustrated by shared accounts and mixed-up chats, with a few reporting difficulty tracking personal data: *"I don't know whose phone I downloaded something on... I'll have to check everyone's phone... who had this photo, who had this text"* (D33). Everyday interface features such as notifications further heightened privacy discomfort by exposing private conversations, leading many dependents to disable them. A few families also reported *"algorithmic mixing"* (M8), where one person's activity reshaped content and ads for others on the same device. In immigrant households, financial constraints and cultural expectations sustained device sharing and intensified its vulnerabilities.

Some parents asserted authority by uninstalling apps, particularly games and social platforms. Financial responsibility was frequently invoked to justify parental control over devices (e.g., *"we pay for it"*), and thus full monitoring au-

thority. While Kumar et al. [58] describe younger dependents' pragmatic acceptance of this logic, dependents in our study, spanning a much wider age range, recognized it but described it as uneasy and conflict-laden.

Dependents' comfort with device sharing varied, revealing three recurring patterns: (1) open discomfort, (2) pragmatic acceptance with protective behaviors, and (3) stated comfort alongside privacy concerns. Most expressed resentment, describing sharing as *"monitoring without consent"* (D26). A few accepted it but minimized privacy risks by limiting activity or keeping *"nothing personal"* on shared devices. The few who described sharing as "reasonable" or "comfortable" often voiced a desire for privacy reported protective strategies. Some suggested that such comfort reflected cultural expectations rather than genuine preference, noting that *"our culture is like very much collectivist, so we want to share"* (D28).

5.2.3 Child Originated Threats

Seemingly low-stake risks initiated by dependents can escalate to household-level S&P threats due to the interconnected nature of banking, school, social media, and email accounts. We group these into two main harms:

Reputational and Cultural Privacy Harms: A few dependents' actions on shared parental devices unintentionally affected parents' reputations, causing embarrassment, serious professional and sociocultural harm. For example, in one family, a child texted the mother's boss, *"I love you"* (D20). While such incidents could pose professional risks in any context, consequences may be amplified for women from conservative immigrant backgrounds who face stricter modesty norms and greater reputational harm if these norms are perceived to be violated, even accidentally [4]. Such incidents may be read as inappropriate behavior, affecting reputation within communities in Canada or in their home country [4].

Additionally, shared devices often caused boundary spillover when family members encountered or disclosed one another's morally sensitive content, violating culturally and religiously defined privacy norms. A few parents described dependents' actions leading to loss of control over personal images as especially serious; as M16 explained, *"I don't reveal my face, [yet] my kid put my picture on display on WhatsApp"* — a strong and irreversible privacy breach, particularly for Muslim Women [30]. In shared-device contexts, dependents' easy access to family photos, accounts, or unlocked sessions enabled such disclosures without parental awareness or consent (also see Section 6.1). Shared access also exposed dependents to content they were not meant to see, as sharing often made parents' private or unfiltered media visible across users. For example, a teenager (S40) was shocked to encounter a romantic photo of his parents that is strictly private in their culture and religion.

Risk Underestimation and Informal Workarounds: Financial risk emerged as the most frequently cited security concern, with nearly all parents reporting heightened vigilance around financial data or protective avoidance behaviors. Yet, primary email accounts linked to banking often remained persistently logged in on shared devices and were not perceived as vulnerabilities: *"Banking apps automatically close... regarding my email address, you can open it here, you can open it in the other device, it's already saved"* (F3).

This narrow financial threat model became especially concerning in shared-device households, where dependents' actions could escalate into household-wide financial risk. One family described a shared-device being hacked after a child downloaded malware, raising fears of financial data exposure: *"That was a huge privacy concern... My dad was scared that they might take some bank information"* (S36). Risks were further compounded when parents were unaware of their children's risky workarounds. A few dependents used concealment apps that created hidden spaces parents could not easily monitor, including *"a fake calculator app... If you put in... a specific password, it opens like a hidden photos app"* (S36). Although intended to create privacy, these workarounds introduced risks that parents could neither assess or regulate.

5.2.4 S&P Workarounds for Device-Sharing

We identified five overarching S&P challenges faced by immigrant families: account compromise, intra-family privacy erosion, social and reputational harms, governance breakdown, and external exploitation. Families addressed these risks through technical controls and behavioral or social strategies. In this section, we focus on the behavioral dimensions of these challenges, while a full summary of all identified risks and practices is provided in Figure 3 in Appendix D.

Families relied on risk-avoidance and ad hoc concealment tactics to manage S&P on shared devices. Rather than using negotiated boundaries or system-level multi-user controls, most managed privacy behaviorally by avoiding personal storage, closing apps, or erasing traces before sharing devices. A few described open, trust-based sharing models, where members freely accessed one another's data, blurring boundaries between consent, convenience, and surveillance.

Language as a privacy tool: A few reported language as a privacy tool in shared-device homes by both parties to obscure content from the other; Parents noted dependents did not understand their local language: *"now the only code wording [on devices] we do is in Urdu" (M8)*, while dependents described feeling safer only because their mother *"can't really speak English... so she didn't really understand what anything meant" (S36)* after she opened a group chat.

Dependents: Dependents emphasized personal chats, photos, and privacy-sensitive browsing as key concerns on shared devices [107]. Our findings on password sharing align with prior work [98, 105]. Since structural controls for device separation were insufficient, almost all dependents routinely closed apps, cleared histories, and logged out of accounts before returning devices to another family member, while some children adopted risky workarounds (e.g., decoy or third-party

vault apps), introducing further risks.

Parents: Almost all parents prioritized protecting communication content, financial data, and authentication credentials on shared devices, reflecting fears of social exposure and data compromise. Few relied on built-in safeguards such as separate accounts, passwords, or safer browsing settings for multi-user use; instead, almost all protections were enacted behaviorally through monitoring, oversight, manual content vetting, and reactive app bans. Similar to dependents' behaviors, a few parents also reported closing all open apps before handing over a device and limiting use to a single browser so that nothing private remained accessible.

Social Regulation: Some parents maintained dependents' online safety by permitting social platforms considered "not trending" among peers. For example, F2 said, *"[My daughter] wants her account on TikTok and Snapchat. She doesn't want her account on YouTube... YouTube is not trending so it's safe on our end."* Parents perceived three benefits of this strategy: reduced peer influence on values, lessened interests in public posting due to social irrelevance, and lowered screen-time. This platform curation made shared-device use more manageable by limiting risky disclosure and co-use conflicts. However, most children responded to this by using install-delete app cycles: *"I delete the app... then every time I have to use it, I install it again"* (D26).

5.2.5 Learning Security the Hard Way

Only a few families configured security protections proactively; most adopted safeguards only after harm had already occurred. Safety was often equated with the absence of prior incidents, as one parent explained: *"I guess because nothing bad has happened so far. That's why I think that it's safe"* (M12), a view echoed by almost all participants. When incidents occurred, families typically responded reactively by removing or avoiding the implicated app, account, or access point; for example, deleting WhatsApp Web, restricting chat access, or creating separate laptop accounts. These responses reflected inconsistent, reactive strategies rather than systematic shared-device security practices.

Even technologically capable parents acknowledged limits to control: *"Those things you can't control fully... once in a while those things do pop up"* (M18). These responses reflect a shared-device threat model in which security was framed as controlling dependents' access rather than preventing external compromise. Protection was sometimes reduced to a single visible safeguard, most commonly antivirus software: *"It's just having the antivirus on the laptop, I feel that that's enough, more than enough"* (M12). Notably, several families sought assistance through culturally familiar networks (e.g., relatives or friends with technical expertise), often to secure shared household devices, reflecting culturally shaped trust patterns and a limited reliance on formal institutional support. These findings expose a mismatch between shared-device realities and current protections, highlighting a need for closer examination of how existing tools perform and what safer sharing should look like, which we discuss further.

5.3 (RQ3) Safe Sharing

> *Our culture is like very much collectivist, so we want to share. (D28)*

This quote reflects families' visions of safe sharing are grounded in collectivist norms, seeking a balance between safety, privacy, while continuing sharing. We map our findings based on the effectiveness of current mechanisms (5.3.1), limitations of current S&P tools for device sharing (5.3.2) , advice for families (5.3.3) and design needs required to support safer device sharing (5.3.4).

5.3.1 Mechanisms That Support Device-Sharing

Dependents: Almost all dependents strongly appreciated separation mechanisms that help manage visibility on shared devices, enabling privacy without requiring fully separate devices. Separate profiles on laptops were appreciated by most, as D21 explained, *"having different profiles on like the devices we share gives us each our own kind of privacy."* On phones, a few dependents also praised lightweight safeguards that reduced accidental exposure during brief handoffs, including auto-lock and short lock timers: *"Passwords, the locks, so the automatically lock thing... setting your phone to lock after like thirty seconds"* (D28), as well as app-level biometrics such as *"fingerprint on apps"* (M19), or hidden photos folders. These were also the most requested features, further elaborated in Section 5.3.2. These mechanisms were valued because they enabled privacy within ongoing device sharing rather than requiring full device separation.

Parents: Most parents described relying primarily on built-in device features and parental controls to manage shared-device use, pointing to app restrictions, passcodes, remote access to wi-fi toggling, and age-based filtering (eg, YouTube Kids) as practical safeguards. A few parents with experience across ecosystems consistently described Android Family Link as the most reliable tool because enforcement was immediate and difficult to bypass: *"the enforcement of the controls is much stronger... the moment you push it out in Android it applies to the devices right away"* (F4). They also valued its combination of monitoring and real-time control, including bedtime and Wi-Fi shutdowns: *"I can actually switch off their device right now... I can control the time that the person is on Instagram, the time that the person is on Roblox... you can actually remove Wi-Fi"* (M18).

A few parents also valued signals that surfaced misuse without constant monitoring, such as alerts after failed login attempts, described by one parent as a feature where repeated password attempts *"takes your picture... [and] gives you a notification on your email"* (M12). Hinting features that enabled remote management of shared devices. Some participants highlighted Canada-specific protections, noting

scam-call filtering as a meaningful built-in defense after migration: *"once I moved here... I immediately start receiving this fraud calls... it's built-in... it shows it's fraud"* (M19).

5.3.2 Participant Reported Device Limitations

Despite this appreciation, almost all emphasized that no single tool met all their sharing needs. As one parent summarized, different platforms each "do some things well," but none "do everything," which we further discuss below.

Dependents: Across almost all dependents' accounts, no built-in feature made shared devices feel safe; notably, most did not associate "safety" with antivirus or stronger settings, but with privacy from household monitoring and judgment and with limiting visibility. When asked what helped in device sharing, responses were often blunt: *"nothing makes device sharing feel safer"* (D26, S38). Most dependents reported feeling threatened by everyday visibility: notifications, synced accounts, search and streaming history logs, and message previews exposed private conversations to parents, *"what makes [device sharing] hard is my dad looking through my Gmail messages"* (D26). Dependents proposed data separation measures, such as app-specific passwords or biometric logins, Face ID, security questions, devices to allow only specific people access, or, ultimately, *"a separate device... which no one can access"* (D26).

Parents: Across families, most parents reported that existing parental controls were often hard to configure, burdensome to maintain, and poorly suited to shared-device use, leading most parents to abandon them despite the need. Notably, almost all were highly educated and digitally competent yet still reported fatigue and confusion. Most found available controls fragmented and difficult to use. For example, one parent described the complications of monitoring in the presence of many apps and users, making it difficult to attribute usage to specific individuals and to enforce user-specific limits: *"if there is any app to find out how much a person uses... that would be much more helpful"* (F6).

Some described delays between configuring restrictions and their actual enforcement, reducing usefulness in time-sensitive situations. Almost all parents who used parental controls (e.g., Family Link) wanted greater granularity. Although F4 and M18 viewed Android Family Link as better than alternatives, they still noted major flaws. A few others reported being unable to reliably enforce screen-time, and that dependents quickly learned to bypass restrictions, like "factory resetting" network connections to reset Wi-Fi controls. Content filtering was also described as insufficient by some, with even child-friendly media surfacing sexual or violent themes. One parent with a child under the age of ten explained, *"... watching Sonic game video... Sonic is like pregnant... and someone is beating him... you cannot stop them with a filter... so even these apps are not safe"* (F2). As discussed in Section 5.2.3, parents also struggled to maintain boundaries and content separation on shared devices. Managing parental controls were described as tiring or stressful to manage, largely because single controls could not easily enforce user-specific rules in multi-user households.

5.3.3 Advice for Sharing Devices

When asked, *"What advice do you have for families that share devices?"*, dependents' responses centered on everyday self-restraint and respectful use, emphasizing simple behavioral rules to avoid accidental exposure or conflict. Most dependents emphasized behavioral restraint as central to safe sharing, for generic safety risks such as avoiding "inappropriate" or risky use, while also advising parental figures to give space: *"Just don't look through my messages... don't click bad websites,"* (D26). When asked what counted as "bad," dependents pointed to unverified websites, "culturally inappropriate" apps, and any platforms that enable communication with strangers (S37). Most emphasized "digital hygiene," mutual respect, accessing only what was necessary, and returning the device quickly to avoid exposing others to uncomfortable or risky content. Whereas parents advised conflict-free sharing, framing shared devices as communal household utilities rather than personal possessions: *"Device sharing is like... everyone in the family drives the same car... It's a part of life"* (M17). Most also advocated for clearer rules and reduced functionality for dependents, including limited accounts.

5.3.4 Designing Devices for Safer Sharing

When asked, *"How might current devices be redesigned to support safer device sharing?"*, participants described needs that challenge the dominant single-user model of personal computing. Since phones routinely circulate across family members, participants reported frequent account mix-ups, accidental exposure of private content, and limited ability to enforce boundaries with existing tools. Hence, participants' design requests cluster around five key feature categories. **1)** Identity-aware access that loads the correct family member's device profile (apps, history, and logins) and have role based access levels because *"There might be some stuff that's inappropriate for [parents] to see it's kind of embarrassing."* (D22). **2)** Strict multi-user profile separation, to prevent issues and conflicts explained in Section 5.2.2. **3)** Parental controls unified across operating systems, and catering to limitations of current devices (Section 5.3.2), along with user based activity logs, and an additional culturally configurable aspect *"I wish there were more faith-based security features. 'cause what one thing might be okay in Christianity is totally not okay in Islam, right?"* (M9). **4)** Real-time safety alerts due to risks like accessing another users data, or dependent accessing culturally inappropriate content, explained in Section 5.2.3. Lastly, **5)** Granular privacy controls (requested strongly by dependents) like stealth histories, per-app unlocks, visibility controls for apps etc although these are against the notion of *"If you need that much privacy, you're doing something wrong."* (D33).

6 DISCUSSION

An idealized metaphor for device sharing described by one of our participants is that it should be like sharing a car —a routine and socially neutral activity. However, our participants' lived realities challenge this notion. Across immigrant families, shared devices were not merely functional tools but sites of cultural regulation and family governance. Parents described sharing as "normal, comfortable, and cultural," aligned with having "nothing to hide," yet, also acknowledged its risks discussed in Section 5.2, revealing tensions in practice. Some dismissed privacy as "not even real" to justify unannounced monitoring, reinforcing parental authority in ways dependents found discomforting and disturbing, demonstrating that challenges operated in both directions.

A recurring challenge was disentangling the influence of religiosity, immigrant status, and host-country cultural norms on device sharing practices. Participants often described these factors as deeply intertwined, and many treated religious and cultural values as inseparable. We therefore follow participants' own framing and interpret these influences as mutually constitutive, with religious practice, cultural preservation, and adaptation to a new context often reinforcing one another post-migration.

6.1 Filial Piety, Religiosity and Culture

Consistent with prior work, our findings suggest that device sharing tensions are amplified in collectivist immigrant households not only because sharing is more prevalent, but also due to dynamics such as filial obligation: most dependents felt unable to challenge, forced to comply or expressed discomfort with parental sharing norms [21, 98]. This constrained voice can aggravate privacy harms and disturb family peace, breeding grudges, emotional distance, and hidden workarounds putting entire family at risk (Section 5.2.2).

A prominent theme we found was the influence of faith-based norms on device sharing, extending security concerns beyond technical risks to moral and cultural harms (Section 5.3.4). In our sample, these perceptions were not tied to a single religion but varied with the *intensity of religiosity and cultural values*. Families more invested in religious or cultural traditions articulated stronger faith-based risk notions. Within these households, women's digital privacy was shaped by gendered expectations of modesty, reputation, and self-presentation, intensified in shared-device contexts. Acts such as a dependent posting a mother's veil-less photo or messaging male colleagues "I love you" were viewed as serious breaches causing lasting reputational harm (Section 5.2.3). Illustrating how shared-device risks can disrupt religious self-presentation boundaries (Section 6.1). Prior work shows that contextual factors and values shape privacy perceptions [12, 20, 74]. Our findings align with prior work on norms of modesty [30]; we found that anxieties about women's online visibility, cross-gender interaction, and reputational harm appeared across religious groups. Device sharing reinforced gendered hierarchies, framing privacy as collective accountability to family rather than individual autonomy [71]. Participants also noted that current parental controls often fail to reflect faith-based distinctions (Section 5.3.4). These findings motivate S&P and HCI research on shared-device designs that better support collectivist and faith-based practices, while carefully avoiding designs that reinforce surveillance.

6.2 Designing for Collective Use

One might argue that many requested features (Section 5.3.4) such as multiple profiles or restricted modes, already exist in commercial devices such as Android multi-user profiles, Xiaomi/Redmi Second Space, and Google Family Link parental controls. However, our findings show the core issue is not absence but poor usability and misalignment with household practices. Parents struggled to configure and sustain controls, and dependents experienced privacy mechanisms as insufficient or intrusive. Thus, families gravitated toward social and contextual strategies (e.g., language-based obfuscation, social regulation, monitoring). This gap reflects tensions between single-owner device assumptions and collective device use, alongside knowledge-attitude-behavior barriers [7]. Prior work in Bangladesh similarly shows that available privacy and security features are often underused when they are difficult to configure or misaligned with everyday practices [6, 35, 79]. This highlights a granularity challenge: parents wanted controls that were flexible enough to reflect family-specific needs, but not so detailed that they became difficult to manage [99]. One possible direction is to preset profile and parental-control templates that offer adjustable starting points, reducing setup burden while preserving flexibility. Device sharing is not unique to immigrant families and extends to lower-income or resource-constrained households globally, even in the west [24, 53]. Our sample skews relatively tech-savvy and affluent, with roughly half of households reporting incomes above $100,000 CAD. The fact that these participants still struggled with existing privacy and device sharing features suggests that our findings may underestimate the challenges faced by less tech-savvy or lower-income immigrant households. Improving shared-device security therefore requires not only more features, but features that are usable and contextually informed. Collectivist households act as indicators of failures in single-user security models, as particularly vulnerable or extreme cases that function as canaries that expose structural flaws and push toward more globalized, collective design, similar to how the "curb effect" in accessibility research shows that designing for people with disabilities benefits broader populations [22].

6.3 From Challenges to Goal State

Our findings suggest that tensions in immigrant shared-device households reflect mismatches between institutional technol-

Table 2: Mapping of Device-Sharing Challenges, Participant Articulated Desires, and the Actual Underlying Needs.

Experienced Problems		Articulated Desires		True Underlying Need
Account compromise via shared access	→	Multi-user profiles on phones	→	Each user's account and data remain isolated
Intra-household privacy erosion	→	Trust-tiered access control within families	→	Personal content remains protected during sharing
Sociocultural harms	→	Faith-aligned content filtering and governance	→	Avoidance of culturally or morally conflicting exposure
Governance gaps in child oversight	→	Remote child-device management	→	Stronger and easier parental oversight of child activity
Cross-user actions not attributable	→	Login approval prompts; Per user activity logs	→	Unsafe or rule-breaking actions remain traceable
External exploitation and financial risk	→	Proactive risk alerts on sensitive activity	→	High-impact risks are detected without constant monitoring
Relational surveillance conflict	→	Stealth history and discreet usage masking	→	Family members cannot monitor each other's activity
Unsafe apps / data compromise	→	App safety ratings in app store	→	Avoidance of unsafe or deceptive downloads

ogy assumptions and everyday family practices. We found that parents struggled to balance home-culture values with Canadian social norms consistent with prior work [98] and sharing disrupted these contextual boundaries [72, 98]. Beyond physical migration, parents described a form of digital immigration [100]: learning to navigate a technologically dense institutional ecosystem (schools, platforms, services) of Canada, while raising children who easily embedded with it. Participants across education levels reported similar difficulties, suggesting these challenges are not limited to some.

A central tension was the divergence between parental and dependent goals: parents sought visibility and control to uphold safety and moral norms, while dependents wanted bounded autonomy and separation of activity on shared devices. These goals created a persistent tension between oversight and privacy. Even same feature requests encoded opposing intentions. The misfit between individual-centric devices and family use, where "safety" and "privacy" differ by role, requires mechanisms that support parental assurance without undermining dependents' privacy.

Some feature requests, such as app-store safety ratings for children, convey safety concerns that devices do not support. Although difficult to standardize, the underlying need is clearer: parents want visibility into what apps enable what privileges for dependents, what data they access, and how they affect shared-device risks. More actionable approaches to solve this problem could include standardized pre-installation disclosures of data sharing, communication capabilities, and exposure risks on the app store. Interpreting requests at this intent level helps designers address true underlying needs. The goal is not a single "best feature," as there is likely no single "sweet spot," and trade-offs are unavoidable. Hence, the aim is reducing device sharing tensions and preserving family bonds and safety.

We therefore recommend that participant design needs (Section 5.3.4) should be understood not as isolated feature checklist but as expressions of a desired goal state shaped by the challenges mentioned in Section 5.2. We map these desired features and challenges onto each other to find out the actual goal state of our participants. The mapping (Table 2) shows participants' stated desires sometimes exceeded what is structurally required for safer sharing. Some requested mechanisms illustrate how this goal could materially improve safety. True multi-user profiles with automatic switching for example, would reduce account mixing and unintended cross-user exposure. A tiered visibility model: where high-sensitivity categories (messaging, photos, banking) are user-locked while others (browser, camera, dialpad) remain shared, could accommodate both dependent privacy and parental oversight within the same session, without forcing a binary choice. Contextual alerts for sensitive actions or account changes could provide parental assurance without continuous surveillance. The goal state is design grounded in underlying challenges.

7 Conclusion and Future Work

Designing for marginalized or extreme users often produces solutions that benefits broader populations. Immigrant shared-device households experience intensified forms of device sharing risks that reveal the limitations of single-user design assumptions, positioning them as informative edge use cases. We argue that designing systems that support safe sharing would therefore benefit not only collectivist immigrant families, but also mainstream users who share devices episodically and facing similar risks of cross-account exposure and privacy conflicts. Addressing S&P challenges in immigrant shared-device households has implications beyond this population. Revisiting our research questions, these challenges stem less from awareness gaps than from mismatches between collectivist sharing practices and single-user device models. Safer shared use therefore requires stronger system-level privacy protections and more usable features that move beyond single-user assumptions to support multi-user, culturally situated device contexts. Further research across diverse socioeconomic, immigrant, and religious setting is needed to disentangle culturally specific dynamics from broader multi-user constraints, clarify resulting design requirements, and assess how these insights generalize across wider device sharing populations.

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, page 451–466, USA, 2019. USENIX Association.

[2] Norah Abokhodair. Transmigrant Saudi Arabian Youth and Social Media: Privacy, Intimacy and Freedom of Expression. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '15, page 187–190, New York, NY, USA, 2015. Association for Computing Machinery. doi.org/10.1145/2702613.2702629.

[3] Norah Abokhodair and Sarah Vieweg. Privacy & Social Media in the Context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, page 672–683, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2901790.2901873.

[4] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, strangers, and the FBI: online privacy concerns and experiences of muslim-american women. In *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security*, SOUPS'22, USA, 2022. USENIX Association.

[5] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), December 2017. doi.org/10.1145/3134652.

[6] Syed Ishtiaque Ahmed, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. "Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery. doi.org/10.1145/3290605.3300410.

[7] Icek Ajzen. Attitudes, Personality, and Behavior. In Wolfgang Stroebe and Miles Hewstone, editors, *Attitudes and the Attitude–Behavior Relation: Reasoned and Automatic Processes*, volume 11 of *European Review of Social Psychology*, pages 1–33. Wiley, 2000.

[8] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-based Privacy and Security for Mobile Smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3544549.3585904.

[9] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW1), April 2022. doi.org/10.1145/3512904.

[10] Mahdi Nasrullah Al-Ameen, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna. "We, three brothers have always known everything of each other": A Cross-cultural Study of Sharing Digital Devices and Online Accounts. *Proceedings on Privacy Enhancing Technologies*, 2021(4):203–224, 2021.

[11] Norah Alqahtani, Steven Furnell, Shirley Atkinson, and Ingo Stengel. Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi Context. In *2017 Internet Technologies and Applications (ITA)*, pages 98–103, 2017.

[12] Irwin Altman. *Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole, Monterey, CA, 1975.

[13] Analytics Insight. Android's Multi-User Mode: Ultimate Solution for Shared Devices. `https://www.analyticsinsight.net/how-to/androids-multi-user-mode-ultimate-solution-for-shared-devices`, February 2025. Accessed: 14 Feb 2026.

[14] Jacquline Angella Smith. "Faith and Fashion: Christian Dress and Identity". 2021. doi.org/10.32920/ryerson.14644872.

[15] Fanni Bányai, Ágnes Zsila, Orsolya Király, Aniko Maraz, Zsuzsanna Elekes, Mark D. Griffiths, et al. Problematic Social Media Use: Results from a Large-Scale Nationally Representative Adolescent Sample. *PLOS ONE*, 12(1):e0169839, 2017.

[16] Thierry Bardini. *Bootstrapping: Douglas Engelbart, coevolution, and the origins of personal computing*. Stanford University Press, USA, 2001.

[17] Thierry Bardini and August T. Horvath. The Social Construction of the Personal Computer User. *Journal of Communication*, 45(3):40–65, 1995.

[18] Timothy Bartkoski, Ellen Lynch, Chelsea Witt, and Cort Rudolph. A Meta-Analysis of Hiring Discrimination Against Muslims and Arabs. *Personnel Assessment and Decisions*, 4(2):Article 1, 2018. `https://scholarworks.bgsu.edu/pad/vol4/iss2/1`.

[19] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 635–654. IEEE, 2024.

[20] Victoria Bellotti and Abigail Sellen. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third Conference on European Conference on Computer-Supported Cooperative Work*, ECSCW'93, page 77–92, USA, 1993. Kluwer Academic Publishers.

[21] Vern L. Bengtson and Petrice S. Oyama. *"Intergenerational Solidarity and Conflict"*, pages 35–52. Palgrave Macmillan US, New York, 2010. doi.org/10.1057/9780230115484$_3$.

[22] Angela Glover Blackwell. The Curb-Cut Effect. *Stanford Social Innovation Review*, 15(1):28–33, 2016. doi.org/10.48558/YVMS-CC96.

[23] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[24] A. J. Bernheim Brush and Kori M. Inkpen. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In *UbiComp 2007: Ubiquitous Computing*, pages 109–126, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. doi.org/10.1007/978-3-540-74853-3$_7$.

[25] Jenna Burrell. Evaluating Shared Access: Social Equality and the Circulation of Mobile Phones in Rural Uganda. *Journal of Computer-Mediated Communication*, 15(2):230–250, 2010.

[26] Soo Fei Chuah. When mobile phone use becomes problematic: the influence of self, parents and peers on adolescents' mobile phone behavior in Singapore and Malaysia, 2018.

[27] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3173574.3174158.

[28] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 19–35, USA, 2014. USENIX Association.

[29] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi 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*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery. doi.org/10.1145/1837110.1837130.

[30] Lakshmi Devi and Manvinder Kaur. Purdah or Ghunghat, a Powerful Means to Control Women: A Study of Rural Muslim and Non-Muslim Women in Western Uttar Pradesh, India. *Indian Journal of Gender Studies*, 26(3):336–349, 2019. doi.org/10.1177/0971521519861162.

[31] Serge Egelman, A. J. Bernheim Brush, and Kori M. Inkpen. Family Accounts: A New Paradigm for User Accounts Within the Home Environment. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW '08)*, pages 669–678. ACM, 2008. doi.org/10.1145/1460563.1460666.

[32] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith 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*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery. doi.org/10.1145/3290605.3300764.

[33] Victoria M. Esses. Prejudice and Discrimination Toward Immigrants. *Annual Review of Psychology*, 72:503–531, 2021. doi.org/10.1146/annurev-psych-080520-102803.

[34] Virginia Eubanks. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, Inc., USA, 2018.

[35] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, 7(12), 2017. doi.org/10.1186/s13673-017-0093-6.

[36] Tom Fairless. Immigration Backlashes Spread Around the World, July 2023. `https://www.wsj.com/world/immigration-backlashes-spread-around-the-world-142124bc`.

[37] Helen Gardner and Duncan Randall. The effects of the presence or absence of parents on interviews with children. *Nurse Researcher*, 19(2):6–10, 2012. `https://doi.org/10.7748/nr2012.01.19.2.6.c8902`.

[38] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3173574.3173698.

[39] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela 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*, CHI '18, page 1–14, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3173574.3173768.

[40] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–15, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3173574.3173688.

[41] Yasmeen Hashish, Andrea Bunt, and James 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*, CHI '14, page 1797–1806, New York, NY, USA, 2014. Association for Computing Machinery. doi.org/10.1145/2556288.2557128.

[42] Sumair Ijaz Hashmi, Niklas George, Eimaan Saqib, Fatima Ali, Nawaal Siddique, Shafay Kashif, Shahzaib Ali, Nida Ul Habib Bajwa, and Mobin Javed. Training Users to Recognize Persuasion Techniques in Vishing Calls. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3544549.3585823.

[43] N. Havermans, S. Vanassche, and K. Matthijs. Methodological Challenges of Including Children in Family Research: Measurement Equivalence, Selection Bias and Social Desirability. *Child Ind Res*, 8:975–997, 2015.

[44] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Durmuth, Yixin Zou, and M. Angela 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)* , pages 697–716, Los Alamitos, CA, USA, May 2024. IEEE Computer Society. doi.ieeecomputersociety.org/10.1109/SP54263.2024.00027.

[45] Geert Hofstede. Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1), 2011. doi.org/10.9707/2307-0919.1014.

[46] Hofstede Insights. 6D Model of National Culture. https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/, n.d. Accessed: 2026-02-10.

[47] Andrew Gary Darwin Holmes. Researcher positionality – A consideration of its influence and place in qualitative research - A new researcher guide. *Shanlax International Journal of Education*, 8(4):1–10, 2020.

[48] Jack Holt, James Nicholson, and Jan David Smeddinck. From Personal Data to Digital Legacy: Exploring Conflicts in the Sharing, Security and Privacy of Post-mortem Data. In *Proceedings of the Web Conference 2021*, WWW '21, page 2745–2756, New York, NY, USA, 2021. Association for Computing Machinery. doi.org/10.1145/3442381.3450030.

[49] Samia 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*, CHI EA '21, New York, NY, USA, 2021. Association for Computing Machinery. doi.org/10.1145/3411763.3450383.

[50] Samia Ibtasam, Lubna Razaq, Maryam Ayub, Jennifer R. Webster, Syed Ishtiaque Ahmed, and Richard 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.*, 3(CSCW), November 2019. doi.org/10.1145/3359148.

[51] Immigration, Refugees and Citizenship Canada. Fraud targeting newcomers, 2025. https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/newcomers.html.

[52] Interac Corp. Interac survey shows more than half of new Canadian families have been targeted by financial fraud, Nov 8 2023. https://www.interac.ca/en/content/news/interac-survey-shows-more-than-half-of-new-canadian-families-have-been-targeted-by-financial-fraud.

[53] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. Caring About Sharing: Couples' Practices in Single User Device Access. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work*, GROUP '16, page 235–243, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2957276.2957296.

[54] Jeffrey James and Mila Versteeg. Mobile phones in Africa: How much do we really know? *Social Indicators Research*, 84(1):117–126, 2007. doi.org/10.1007/s11205-006-9079-x.

[55] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, page 1647–1650, New York, NY, USA, 2009. Association for Computing Machinery. doi.org/10.1145/1518701.1518953.

[56] Joseph 'Jofish' Kaye. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 2619–2622, New York, NY, USA, 2011. Association for Computing Machinery. doi.org/10.1145/1978942.1979324.

[57] Lindah Kotut and Hummd Alikhan. "Things on the Ground are Different": Utility, Survival and Ethics in Multi-Device Ownership and Smartphone Sharing Contexts. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery. doi.org/10.1145/3613904.3642874.

[58] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), December 2017. doi.org/10.1145/3134699.

[59] Carolyn A. Lin. Exploring personal computer adoption dynamics. *Journal of Broadcasting & Electronic Media*, 42(1):95–112, 1998.

[60] Yunxin Liu, Ahmad Rahmati, Yuanhe Huang, Hyukjae Jang, Lin Zhong, Yongguang Zhang, and Shensheng Zhang. xShare: supporting impromptu sharing of mobile phones. In *Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services*, MobiSys '09, page 15–28, New York, NY, USA, 2009. Association for Computing Machinery. doi.org/10.1145/1555816.1555819.

[61] Sonia Livingstone, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud. In Their Own Words: What Bothers Children Online? *European Journal of Communication*, 29(3):271–288, 2014.

[62] Mirca Madianou and Daniel Miller. *Migration and New Media: Transnational Families and Polymedia*. Routledge, 1 edition, 2012. doi.org/10.4324/9780203154236.

[63] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 5921–5932, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2858036.2858051.

[64] Nicole Meng-Schneider, Rabia Yasa Kostas, Kami Vaniea, and Maria K Wolters. Multi-User Smart Speakers - A Narrative Review of Concerns and Problematic Interactions. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3544549.3585689.

[65] Mario Millán-Franco, Luis Gómez-Jacinto, Isabel Hombrados-Mendieta, Felipe González-Castro, and Alba García-Cid. The Effect of Length of Residence and Geographical Origin on the Social Inclusion of Immigrants. *Psychosocial Intervention*, 28(3):119–130, 2019. doi.org/10.5093/pi2019a10.

[66] Phoebe Moh, Andrew Yang, Nathan Malkin, and Michelle L. Mazurek. Understanding how people share passwords. In *Proceedings of the Twentieth USENIX Conference on Usable Privacy and Security*, SOUPS '24, USA, 2024. USENIX Association.

[67] Laura L. Murphy and Alexandra E. Priebe. "My co-wife can borrow my mobile phone!": Gendered Geographies of Cell Phone Usage and Significance for Rural Kenyans. *Gender, Technology and Development*, 15(1):1–23, 2011.

[68] Maryam Mustafa, Abdul Moeed Asad, Shehrbano Hassan, Urooj Haider, Zainab Durrani, and Katharina Krombholz. Pakistani Teens and Privacy - How Gender Disparities, Religion and Family Values Impact the Privacy Design Space. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 195–209, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3576915.3623087.

[69] Maryam Mustafa, Shaimaa Lazem, Ebtisam Alabdulqader, Kentaro Toyama, Sharifa Sultana, Samia Ibtasam, Richard Anderson, and Syed Ishtiaque Ahmed. IslamicHCI: Designing with and within Muslim Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI EA '20, page 1–8, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3334480.3375151.

[70] Electra Nanou. How to Add Multiple User Profiles and Use Guest Mode on Your Android phone. `https://www.makeuseof.com/add-user-profiles-guest-mode-android/`, April 2023. Accessed: 14 Feb 2026.

[71] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. "Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond W.E.I.R.D. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery. doi.org/10.1145/3491102.3501883.

[72] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA, 2009.

[73] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. The Burden of Ending Online Account Sharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3313831.3376632.

[74] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, page 129–136, New York, NY, USA, 2003. Association for Computing Machinery. doi.org/10.1145/642611.642635.

[75] Tapan S. Parikh and Kaushik Ghosh. Understanding and Designing for Intermediated Information Tasks in India. *IEEE Pervasive Computing*, 5(2):32–39, April 2006. doi.org/10.1109/MPRV.2006.41.

[76] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. In *Proceedings of the New Security Paradigms Workshop*, NSPW '19, page 1–15, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3368860.3368861.

[77] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, and Mahdi Nasrullah Al-Ameen. A First Look Into Parental Strategies, and Challenges Around Children's Device Usage in Urban Nepal. In Masaaki Kurosu and Akira Hashizume, editors, *Human-Computer Interaction. HCII 2025*, volume 15770 of *Lecture Notes in Computer Science*, pages 277–296, Cham, 2025. Springer.

[78] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. A Deep Dive into User's Preferences and Behavior around Mobile Phone Sharing. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW1), April 2023. doi.org/10.1145/3579595.

[79] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security*, SOUPS '19, pages 319–338, Santa Clara, CA, August 2019. USENIX Association.

[80] Aunam Quyoum, Mark Wong, Sebati Ghosh, and Siamak F. Shahandashti. Minoritised ethnic people's security and privacy concerns and responses towards essential online services. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security*, SOUPS '25, USA, 2025. USENIX Association.

[81] Rahat Jahangir Rony and Nova Ahmed. Teens Online Behavior and Support Interventions in Bangladesh. *ACM J. Comput. Sustain. Soc.*, 3(1), January 2025. doi.org/10.1145/3704813.

[82] Steven Ruggles and Misty Heggeness. Intergenerational Coresidence in Developing Countries. *Population and Development Review*, 34(2):253–281, 2008. doi.org/10.1111/j.1728-4457.2008.00219.x.

[83] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchil. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS '18, page 127–142, USA, 2018. USENIX Association.

[84] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. Intermediated technology use in developing communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 2583–2592, New York, NY, USA, 2010. Association for Computing Machinery. doi.org/10.1145/1753326.1753718.

[85] Shruti Sannon and Andrea Forte. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), November 2022. doi.org/10.1145/3555556.

[86] Abhinaya S.B., Agrawal Agrawal, Yaxing Yao, Yixin Zou, and Anupam Das. "What are they gonna do with my data?": Privacy Expectations, Concerns, and Behaviors in Virtual Reality. *Proc. Privacy Enhancing Technologies (PoPETs)*, 2025(1):58–77, 2025. doi.org/10.56553/popets-2025-0005.

[87] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, page 895–904, New York, NY, USA, 2007. Association for Computing Machinery. doi.org/10.1145/1240624.1240759.

[88] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They Look at Vulnerability and Use That to Abuse You'': Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 323–340, Boston, MA, August 2022. USENIX Association.

[89] Statistics Canada. Immigrant Population in Canada, 2021 Census, 2022. https://www12.statcan.gc.ca/census-recensement/2021/as-sa/98-200-x/2021006/98-200-x2021006-eng.cfm.

[90] Molly Wright Steenson and Jonathan Donner. Beyond the Personal and Private: Modes of Mobile Phone Sharing in Urban India. In Scott W. Campbell and Rich Ling, editors, *The Reconstruction of Space and Time: Mobile Communication Practices*, pages 231–250. Transaction Publishers, 2009.

[91] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021. doi.org/10.1145/3479526.

[92] A. Strauss and J. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage, Thousand Oaks, CA, 1990.

[93] Sarah Tabassum, Nishka Mathew, and Cori Faklaris. Privacy on the Move: Understanding Educational Migrants' Social Media Practices through the Lens of Communication Privacy Management Theory. In *Proceedings of the 2025 ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies*, COMPASS '25, page 1–18, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3715335.3735453.

[94] Hiromi Taniguchi and Gayle Kaufman. Family, Collectivism, and Loneliness from a Cross-Country Perspective. *Applied Research in Quality of Life*, 17:1555–1581, 2022. doi.org/10.1007/s11482-021-09978-8.

[95] The Canadian Press. Canadians targeted 'more aggressively' by fraud calls than Americans, study suggests. *The Globe and Mail*, May 2023. https://www.theglobeandmail.com/business/article-canadians-targeted-more-aggressively-by-fraud-calls-than-americans/.

[96] Ronald L. Thompson, Christopher A. Higgins, and Jane M. Howell. Personal computing: toward a conceptual model of utilization. *MIS Q.*, 15(1):125–143, March 1991. doi.org/10.2307/249443.

[97] Mindy Tran, Collins W. Munyendo, Harshini Sri Ramulu, Rachel Gonzalez Rodriguez, Luisa Ball Schnell, Cora Sula, Lucy Simko, and Yasemin 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)*, pages 617–634, 2024.

[98] Warda Usman, John Sadik, Taha, Ran Elgedawy, Scott Ruoti, and Daniel Zappala. Security and Privacy Experiences of First- and Second-Generation Pakistani Immigrants to the US: Perceptions, Practices, Challenges, and Parent-Child Dynamics. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 2284–2302, 2025. doi.org/10.1109/SP61157.2025.00031.

[99] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions about Them to Support Parenting for Online Safety. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021. doi.org/10.1145/3476084.

[100] Qian (Emily) Wang, Michael D. Myers, and David Sundaram. Digital Natives and Digital Immigrants: Towards a Model of Digital Fluency. *Business & Information Systems Engineering*, 5:409–419, 2013.

[101] Mark Weiser. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, 3(3):3–11, July 1999. doi.org/10.1145/329124.329126.

[102] Kayah Williams and Sarita Schoenebeck. African Immigrants User Experience with USCIS.gov: A Critical

Analysis of a Government-Issued Website Related to Immigration. *Proc. ACM Hum.-Comput. Interact.*, 9(7), October 2025. doi.org/10.1145/3757547.

[103] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page 51–69, New York, NY, USA, 2017. Association for Computing Machinery. doi.org/10.1145/2998181.2998352.

[104] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 3919–3930, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2858036.2858317.

[105] Lirong Yuan, Yanxin Chen, Jenny Tang, and Lorrie Faith Cranor. Account Password Sharing in Ordinary Situations and Emergencies: A Comparison Between Young and Older Adults. In *Proceedings of the Twentieth USENIX Conference on Usable Privacy and Security*, SOUPS '24, 2024.

[106] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How Usable Are iOS App Privacy Labels? *Proceedings on Privacy Enhancing Technologies*, 2022(4):204–228, 2022. doi.org/10.56553/popets-2022-0106.

[107] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*, IDC '16, page 388–399, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2930674.2930716.

Appendix

A Ethical Considerations

Participants were reminded that participation was voluntary and that they could withdraw at any time. Parents provided consent for their own participation and for their underaged children, while young adult dependents provided their own consent. As a token of appreciation, each family was remunerated 60 CAD. Compensation was provided to the enrolling adult (a parent or young adult) rather than distributed individually, reflecting the household-based nature of recruitment and the shared time commitment involved in coordinating family participation. We acknowledge that this approach may not fully account for intra-household power dynamics, particularly in collectivist immigrant families where dependents may have limited agency over how compensation is used or allocated.

Participants were informed that their responses would not be shared with family members, and we avoid reporting intra-family identifiable references. We interviewed parents and dependents from the same household separately to reduce social desirability effects [43] and power dynamics [37]. Some dependents expressed this concern directly, asking, *"Will you tell [my parents]?"* and we assured them that their responses would remain confidential and would not be shared with parents. Nonetheless, some younger participants may have withheld information due to concerns about parental exposure, an inherent limitation of family-based research involving minors. To reduce identity-disclosure risks, we anonymized all responses, balancing analytic transparency with participant safety. To limit the potential for intra-family conflict, we minimized contextual details when reporting findings (e.g., country references), and quotes were selected and edited to be sufficiently general to reduce the likelihood of recognition, demographic details abstracted, and participant attributes delinked where needed.

B Screening Form

1. Are you a first-generation immigrant in Canada?
2. How long have you lived in Canada?
3. What is your country of origin?
4. What languages are spoken in your home?
5. Do you live with your immediate family (i.e., spouse and children)?
6. How many children aged 7–25 currently live in your household?
7. Please list the ages of the children living with you who are willing to participate in the study.
8. Do you or your family members share digital devices with one another?
9. Which of the following devices are regularly shared in your household? (Smartphone, Laptop/Desktop, Tablet/iPads, Gaming Console (PlayStation etc.), Smart Watches, E-Readers)
10. Why do you share these devices? (Financial reasons, Convenience (easier to share than switch devices), Safety and moderation for children, Cultural norms (e.g., family expects device sharing), Other)
11. Would at least one parent and one child be willing to participate in a follow-up interview about device sharing at home?
12. Please provide your name and email address or phone number so we can contact you.

C Interview Protocols

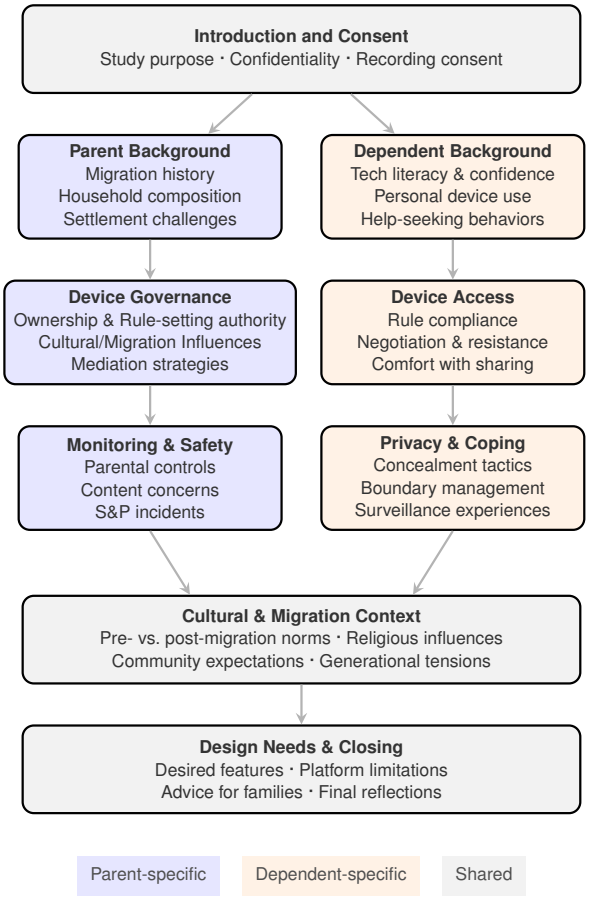


Figure 2: Semi-structured interview protocol with role-specific branches. Parents and dependents followed parallel tracks for device governance and privacy experiences, converging on shared cultural and design themes.

Parent Interview Protocol

Family Background

- Can you briefly introduce yourself?
- Where are you from, and how long have you lived in Canada?
- Who currently lives in your household? Please include their relationship to you and approximate ages.
- What brought you to Canada, and was this decision your own?

Daily Routines and Device Use

- What devices are used in your household, and which ones are shared?
- Do your children have their own devices? When do you think children should get personal devices?
- What are shared devices mainly used for?
- How do you manage privacy, security, and passwords for yourself and your children?
- What online risks concern you most, such as scams, phishing, bullying, or inappropriate content?
- Do you usually take precautions before problems happen or only after something goes wrong?

Digital Literacy and Tech Confidence

- What concerns do you have about the devices or apps your children use, including privacy or security risks such as scams, sharing personal information, unsafe contacts, bullying, or inappropriate content?
- Have you or your child experienced any specific online privacy or safety incident?
- How do you teach or talk to your children about online privacy, security, and safe device use, and are there topics you find difficult to discuss?
- Who in your household usually helps with technology or privacy settings, and how confident are you and your children in using new apps or setting up privacy features?
- Do you feel your children understand online safety more than you? Why or why not?

Device Sharing Practices and Rules

- How were rules or boundaries around device use decided in your household?
- What are the main reasons devices are shared in your home, such as financial reasons, convenience, trust, monitoring, cultural expectations, or children wanting access?
- What rules or boundaries do you have for shared devices, including app locks, blocked content, screen time, logging out, or limits on certain apps?
- How do privacy, trust, and comfort differ when your spouse, children, or other family members use your device?
- What concerns or conflicts have come up when sharing devices, such as feeling watched, judged, denied access, pressured to share, or needing to hide or change device use?
- What tools, advice, or practices do you use to make device sharing safer, more private, and respectful within your household?

Past Incidents and Risks

- What privacy or security problems have you experienced because of device sharing, such as privacy breaches at home, unexpected content discovery, device misuse, scams, hacking, or being misled online?
- What situations make it hardest to maintain privacy boundaries when sharing devices, and have you ever had to confront someone about crossing those boundaries?
- What do you usually do to stay safe online or handle privacy and security concerns, and what advice would you give to a new immigrant family about safe device sharing?

Parental Controls and Supervision

- Who has the most control over devices or accounts in your household, and how are boundaries around access decided?
- What are your rules about what children can or cannot access, and how do you balance trust, supervision, and privacy?
- What strategies do you use to guide or monitor children's device use, such as conversations, casual awareness, parental controls, child accounts, or checking usage and browsing history?

Children's Feelings and Privacy

- How do you think your child feels about sharing devices or accounts with you, especially when they know you may access their device or digital content?
- Has your child ever seemed hesitant to share their device, tried to hide or delete content, or asked you not to open something? How did you respond?
- Do you think your child wants more privacy than you are comfortable giving, and are there any apps, games, or online spaces you are especially concerned about?

Coping Strategies and Workarounds

- What do you or others in your household do to keep information private on shared devices, such as deleting history, hiding apps, using app locks, disabling notifications, using private browsing, or creating secondary accounts?

- What kinds of information or content do you most want to protect, such as financial, immigration, personal, photos, messages, or sensitive browsing activity?
- Which privacy or security tools do people in your household actually use, and which ones feel too difficult, inconvenient, risky, or unnecessary?
- Have any privacy workarounds caused conflict, misunderstanding, or made someone feel like they were hiding something?

Cultural, Social, Religious, and Migration Impacts on Device Sharing

- How have your device-sharing habits, rules, or expectations changed since moving to Canada?
- What parts of migration made device sharing or online safety easier or harder, such as time pressure, fewer supports, financial stress, or fear of consequences?
- How do cultural, social, or religious values shape what devices, apps, or content can be shared in your household?
- Compared to back home, do you feel more or less in control of device sharing and privacy in Canada? Why?
- Do you ever feel pressure, judgment, or misunderstanding around device sharing because of cultural expectations, immigrant experiences, or differences between home and Canadian norms?

Desires, Tools, and Design Ideas

- What features currently make device sharing easier, safer, or harder for your family?
- What kinds of tools or supports would help you feel more in control of privacy and security when sharing devices?
- What features do you wish apps or devices had for families like yours, especially around safe downloads, shared access, app setup, alerts, activity visibility, or reversing mistakes?
- Do you feel current apps, devices, and platforms are designed with families like yours in mind? Why or why not?
- Would you consider using an AI assistant or family management tool to support safer device sharing? Why or why not?
- Is there anything else about device sharing, privacy, or family technology use that we have not asked but should know?

Dependent Interview Protocol

Device Use and Tech Literacy

- What devices do you use at home, such as a phone, tablet, or laptop?
- What do you usually do on these devices, such as games, videos, calling, texting, social media, or schoolwork?
- Who helps set up devices, apps, or privacy settings at home when someone needs help?
- Do adults in your family ever ask you for tech help? What do they usually ask about?
- How confident are you in using new apps or setting up privacy features?

Device-Sharing Practices

- What devices or accounts do you share at home, who do you share them with, and who owns them?
- Which devices feel like yours, and which feel like they belong to everyone?
- Why do you think devices or accounts are shared in your family, such as cost, convenience, trust, rules, or parental control?
- How do you and your family handle sharing issues, such as passwords, screen-time limits, location tracking, shared accounts, or joint logins?
- How do you feel when parents, siblings, or friends use your device, or when you use theirs?

Rules, Power, Trust, and Negotiation

- What spoken or unspoken rules does your family have about sharing devices, accounts, passwords, or screen time?
- Who makes the technology rules at home, who has the most control over devices, and are the rules different for parents, children, older siblings, or younger siblings?
- How do you ask for permission to use someone else's device, and how is sharing usually managed in practice?
- Are there things your parents allow or do not allow you to do on shared devices, and what happens when you do not want to follow those rules?
- Who do you trust most or least with your device, and how do you decide whether something is safe, such as when a friend sends you a link?

Challenges and Worries

- What are the best and worst parts of sharing devices with family?
- Has device sharing ever caused conflict, misunderstanding, embarrassment, or gotten you in trouble? What happened?
- What is the most stressful privacy problem you have faced while sharing devices?
- Do you ever feel watched, judged, or unable to question rules about what you do online?

Accidental Exposure and Incidents

- Have you ever accidentally seen something on a family member's device that was scary, confusing, private, or unexpected? What happened?
- Do you ever worry that your parents or family members might accidentally see your private information, messages, searches, or app activity?
- If someone asks you not to open something on their device, how do you handle that, especially if you feel curious, worried, or suspicious?

Uncomfortable Experiences

- Have you ever seen, received, or found something on a device that scared you, confused you, or made you uncomfortable?
- Has anyone opened your messages, photos, tabs, or other private content without asking, or have you worried about being judged because of your device content?
- Have you or someone in your family ever been scammed, hacked, misled online, or affected by something unsafe online?

Privacy Experiences and Boundaries

- Who teaches you about privacy, security, and online risks, and how is this different at school compared to at home?
- Do you ever help your parents understand apps, security features, scams, fake news, AI videos, or other online risks?
- Do you feel you understand online safety more than your parents? Why or why not?
- How comfortable do you feel sharing devices with family or friends, and do you feel you have enough privacy?
- Have you ever asked someone not to access your device, password, account, or content? How did they respond, and did it cause tension?
- What situations make it hardest to keep privacy boundaries, especially as part of an immigrant family?

Mitigations and Workarounds

- What strategies do you or your family use to stay safe or keep things private on shared devices?
- What privacy or security features do you actually use, such as passwords, two-factor authentication, app locks, device locks, location settings, private browsing, hidden folders, guest modes, or password managers?
- Do you ever avoid certain apps or content, disable notifications, log out quickly, delete history, use secondary accounts, or hide a device to protect your privacy?
- Where did you learn these strategies, and which ones do you rely on most?
- Have any of these strategies caused misunderstandings, felt difficult to use, or made others think you were hiding something?

- Where do you learn about privacy and online safety, such as school, home, Google, YouTube, friends, siblings, or ChatGPT?

Parents' Perspectives

- How do you think your parents feel about sharing their devices or accounts with you, and do they seem to trust you with their digital content?
- Have your parents ever seemed hesitant, upset, or set limits when letting you use their device? How did you respond?

Cultural and Social Norms

- Are the digital rules in your home similar to or different from your friends' families?
- How do friends, family, cultural values, or religious beliefs shape what is okay to do online?
- Have your digital rules, privacy, or device-sharing practices changed since moving to Canada?
- Do you feel more or less in control of your digital privacy now, and are there topics you feel unsure or hesitant to discuss with your parents?

Desired Tools, Support, and Design Ideas

- What advice would you give for sharing devices in a safe, respectful, and private way at home?
- What features currently make device sharing easier, safer, or harder for you?
- If you could redesign a phone, laptop, or app for families who share devices, what features would you add, such as selective screen sharing, extra locks for certain apps, privacy tips, or easier organization?
- Would you trust an AI helper or family tool that gives privacy advice, auto-locks apps, or helps manage shared-device safety? Why or why not?
- Is there anything we did not ask that you think is important about sharing devices or staying private?

D INSIGHT SUMMARIES

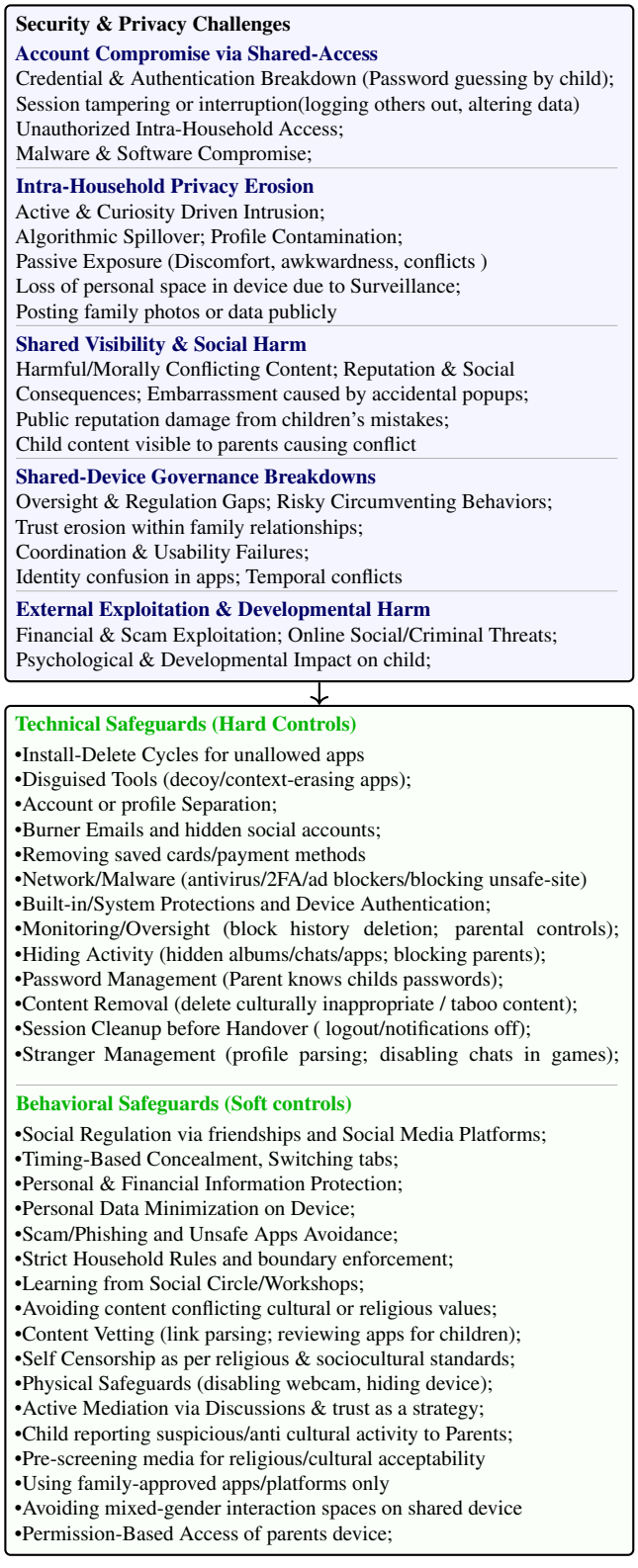


Figure 3: Security and privacy challenges and safeguards in shared-device households.

Top-level Category	Sub-Codes	Sample Sub-sub-codes
RQ1: Sociocultural dynamics of device sharing		
Migration effects on Device-Sharing Norms	Home vs. Host Country	increased device dependence in canada; reduced supervision capacity;
	Forced Early Device Provision	device provision out of necessity; provision as stressful;
	Device-Sharing to Regain Oversight	sharing to regain parental control; device sharing as safety strategy;
Devices as Tools for Cultural Transmission	Promoting Religious Practice	device as reward for religion; religious content encouraged;fear of extremism
	Restricting Political Content	blocking politically content; propaganda in games / media
Conditional Ownership and Parental Authority	Device Ownership as Conditional	independent device but supervised; cultural rules; religious rules
	Obedience and Authority Norms	parents have final decision; cultural expectation of compliance; we pay for it;
	App Installation Conflicts	parent uninstalls apps; child reinstalls; repetitive uninstall-install cycles
Moral and Reputational Screening	Reputation and Community Judgment	fear of host community judgment; extended family scrutiny
	Compliance Framed as Morality	compliance is moral; privacy is a privilege; hiding is a guilt signal
	Moral Hygiene of Devices	"bad"; "clean" / digital hygeine ; install-delete cycles; self-censorship
	Romantic and Gendered Restrictions	dating prohibited; hiding romantic interactions; stricter rules for daughters
Power Imbalances and Gendered Control	Fathers as Primary Rule-Makers	father primary rule-maker; scared of father; rules for spouse
	Gendered Issues	spousal surveillance; deleting from trash; stricter monitoring for daughters
Negotiating/Balancing	Home and Host Country Norms	struggling to balance; pressure from home; "becoming more Canadian"; relaxing strictness to avoid conflict; APM instead of rules; "what else can we do?";
RQ2: Security Landscape of Shared-Device Immigrant Households		
New Country, New Threats	Migration-Linked Scam Exposure	scam calls; fraud messages; phishing calls; deportation scam threats; whatsapp fraud; facebook marketplace scams; unfamiliarity with canadian systems
	Account and Credential Compromise	hacking incidents; password breach; shoulder surfing; saved credentials misuse
	Malware and Unsafe Downloads	fake game links; virus after download; unsafe downloads by dependents; unverified apps; ad-based redirects; malware on shared devices
Shared-Device Vulnerabilities	Account Mixing and Confusion	mixed chats; no separate profiles; algorithmic contamination across users
	Notification and Visibility Exposure	notification spillover; synced account exposure; ad personalization spillover
	Access Competition and Conflict	access competition; sharingfrustration; suggestion to get separate device
Dependent-Originated Risks	Reputational and Cultural Privacy Harms	messaging parents' boss; hijab-less images posted; romantic content; violent content
	Financial Escalation	roblox in-app purchases;shared email linked to banking; unauthorized payment use; banking credentials exposed; digital card avoidance
	Risk Underestimation and Workarounds	friend equals safe; decoy appss; trusting links from ads;
External Exploitation and Household Harm	Financial and Scam Exploitation	fraud calls; bank transfer incidents; deportation scams; phishing exploitation
	Psychological and Developmental Harm	distress after violent exposure; sleep disturbance; fear; anxiety about financial data
	Gendered and Cultural Amplification	reputation damage; purdah violation; amplified consequences for women
Security and Privacy Practices	Technical Safeguards	authentication; account separation; vpn; safer browsing settings; antivirus; built-in protections
	Concealment Tactics	trace deletion; session cleanup; incognito mode; install-delete cycles; disguised apps
	Behavioral Risk Avoidance	bad websites; unsafe downloads; public wifi for banking; limiting personal information
	Language as Privacy Tool	using urdu for private content; relying on parents' limited english literacy
RQ3: Effectiveness of Current Devices and Design Considerations		
Mechanisms That Support Sharing	Appreciated Features (Dependents)	separate laptop profiles; auto-lock timers; app-level biometrics; hidden apps
	Appreciated Features (Parents)	android family link; screen-time controls; scam call filtering; remote wifi control
Limitations of Current Devices	Nothing Makes Sharing Feel Safer	no feature provides adequate safety; safety equated with privacy from household
	Visibility Concerns (Dependents)	notification exposure; synced accounts; message previews; algorithmic surveillance
	Parental Control Failures	manual monitoring still required; controls easy to bypass; delayed enforcement;
	Content Filtering Inadequacy	child filters ineffective; filters insufficient for cultural concerns
	Parental Fatigue and Stress	fatigue limiting supervision; stress from device management; information overload;
Advice for Sharing Families	Advice from Dependents	use separate profiles; avoid bad websites; respect others' privacy; separate devices
	Advice from Parents	share without conflict; be a role model; limit children's access;
	Design Needs	multi-profile phones; separate accounts; isolated storage per user; profile auto-loading on login; warnings for unsafe sites; purchase approval prompts;

Table 3: Codebook Sample