

***“Nothing Can Make Device Sharing Feel Safer...”* Privacy and Security Challenges in Collectivist Immigrant Families**

by

S. Shanza

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2026

© S. Shanza 2026

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners. I understand that my thesis may be made electronically available to the public.

Statement of Contributions

Portions of each chapter in this thesis are based on the following peer-reviewed paper published at the 2026 USENIX Symposium on Usable Privacy and Security (SOUPS) in Hannover, Germany:

“Sharing Digital Devices is Normal and Cultural: Privacy and Security Challenges in Collectivist Immigrant Households,” ¹

I am grateful to all three co-authors for their collaboration in developing the paper. I am deeply grateful to my supervisors, Urs Hengartner and Leah Zhang-Kennedy, for their guidance, mentorship, and unwavering support throughout every stage of this research and my graduate studies. I also thank my co-author, Ameemah Humayun for her contributions to qualitative coding and thematic analysis of the dataset. Text from the published manuscript is used throughout this thesis; however, this thesis substantially expands on the published work, and each chapter extends the analysis with additional depth and discussion beyond what appears in the paper.

¹Authors in publication order: S. Shanza, Ameemah Humayun, Urs Hengartner, and Leah Zhang-Kennedy.

Abstract

In collectivist households, sharing digital devices is both a cultural norm and often a material necessity. After migration to more individualistic cultures such as Canada, these sharing practices persist but become entangled with new cultural norms, unfamiliar institutional infrastructures, and highly digitized systems. Immigrant families must adapt to host-country digital life expectations around privacy, safety, schooling, and online services while continuing to uphold home-country norms around family values, moral and collective responsibilities. Devices, in this context become channels through which trust, supervision, autonomy, and cultural expectations are continuously managed and negotiated.

To understand how this negotiation actually plays out, we report findings from a qualitative study of 18 nuclear families, comprising 19 parents and 22 children and young adults, mainly from South Asia. The study examines three intertwined questions: how migration and sociocultural factors shape the security and privacy risks that shared-device households face, how well current devices support or hinder safe sharing once those risks appear, and how can we better design these devices to support safer device sharing. Our findings show that shared-device use exposed families to data breaches, reputational harms, cultural and religious boundary violations, and intergenerational tensions. Moreover, these risks were naturally amplified to household-level concerns because one person’s online activity, account access, or device use could affect any or all other family members.

We find that families often approached shared devices with different goals. Parents sought visibility and control to protect children, preserve cultural and religious values, and manage safety in an unfamiliar digital environment. Children, in contrast, sought autonomy and ways to keep parts of their digital lives separate while still participating in device sharing household practices. Families used ad hoc and reactive strategies to manage these tensions, including monitoring, informal rules, parental control tools, activity concealment, and self censorship practices like keeping devices in a “morally clean” state. However, these strategies were often fragile, easy to workaroud, difficult to sustain, or abandoned when they threatened family harmony.

Our findings reveal a mismatch between single-user device assumptions and collectivist immigrants’ household realities of device sharing. Current devices offer limited support for shared use that can balance parental assurance, child privacy, cultural expectations, and everyday usability. Designing for shared-device contexts is therefore essential for building more inclusive digital infrastructures that not only support multicultural families but also others who rely on device sharing. Like curb cuts designed for wheelchair users that ultimately benefit many others, designing from the marginalized can produce more inclusive technologies for everyone.

Acknowledgements

I have been incredibly fortunate to be supervised by Dr. Leah Zhang-Kennedy and Dr. Urs Hengartner, whose exceptional mentorship, encouragement, and expertise have profoundly shaped my growth as a researcher. Their guidance has challenged me to think critically, pursue impactful research, and continually strive for excellence. Their unwavering support, insightful guidance, and confidence in my abilities have made my graduate journey both rewarding and inspiring.

I would also like to acknowledge an earlier poster based on this research was presented at the University of Waterloo Cybersecurity and Privacy Institute (CPI) Graduate Student Conference in 2025, where it received the Outstanding Interdisciplinary Poster Award sponsored by Rogers Communications Inc. I am sincerely grateful to the Cybersecurity and Privacy Institute (CPI) for the opportunities it created to present, discuss, and refine this work, and to connect with a broader community of cybersecurity and privacy researchers across Ontario.

I am equally thankful for the support of the CrySP Lab and Games Institute, which provided space, resources, and community throughout my graduate studies.

Dedication

To my family, whose love and support have carried me through every stage of this journey. I dedicate this thesis especially to my parents, for their endless sacrifices, and unwavering belief in me. And to my husband, whose patience, unwavering support, and reassurance carried me through the difficult moments of this journey.

Table of Contents

Author’s Declaration	ii
Statement of Contributions	iii
Abstract	iv
Acknowledgements	v
Dedication	vi
List of Figures	x
List of Tables	xi
1 Introduction	1
1.1 Thesis Statement:	4
1.2 Related Publications:	5
1.3 Thesis Organization	6
1.4 Contributions:	8
2 Related Work	10
2.1 Migrants and Security and Privacy Challenges	11
2.2 Device-Sharing in Collectivist Cultures	14

3	Methodology	17
3.1	Participant Recruitment	18
3.2	Interview Protocol	22
3.3	Data Analysis	24
3.4	Positionality Statement	29
3.5	Ethical Considerations	30
4	Limitations	32
5	Findings	34
5.1	(RQ1) Sociocultural Dynamics of Sharing	40
5.1.1	Home Country to Host Country	40
5.1.2	Devices as Tools for Cultural Transmission	41
5.1.3	Migration-Driven Social Regulation	42
5.1.4	“It’s Yours, But Not Really”	43
5.1.5	Gendered, Spousal and Power Dynamics	44
5.1.6	Surveillance, Conflict, and Emotional Strain	45
5.1.7	Negotiating Culture in New Digital Contexts	46
5.1.8	Trust as a Spectrum: From Coercion to Connection	47
5.1.9	Social and Religious Screening of Devices	48
5.2	(RQ2) Shared-Device Security and Privacy Landscape	51
5.2.1	New Country, New Threats	51
5.2.2	One Device, Too Many Users	51
5.2.3	Financial Loss as the Lens for Security	54
5.2.4	Child Originated Threats	55
5.2.5	Security and Privacy Workarounds for Device-Sharing	57
5.2.6	Learning Security the Hard Way	61
5.2.7	School vs at Home Teaching	64

5.2.8	Reverse Mediation:	65
5.2.9	Say-Do Gaps in Privacy Practice	66
5.3	(RQ3) What Makes Sharing Safe	68
5.3.1	Mechanisms That Support Device-Sharing	68
5.3.2	Participant Reported Device Limitations	70
5.3.3	Advice for Sharing Devices	71
5.3.4	Designing Devices for Safer Sharing	72
6	Discussion	74
6.1	Filial Piety, Religiosity and Culture	75
6.2	Teaching Avoidance, Not Understanding	76
6.3	Designing for Collective Use	77
6.4	From Challenges to Goal State	79
6.5	Future Design Directions	81
7	Conclusion and Future Work	83
	References	86
	APPENDICES	107
A	Interview Protocol	108
B	Household Demographics Form	114

List of Figures

3.1	Overview of the Study Procedure.	18
3.2	Summary of Interview Protocol Questions	21
5.1	Terminology for Relative Frequency	34
5.2	Device Sharing S&P Landscape.	39
5.3	S&P Challenges and Safeguards	58

List of Tables

3.1	Screening Form Questions	19
3.2	Codebook Sample for RQ1	26
3.3	Codebook Sample for RQ2	27
3.4	Codebook Sample for RQ3	28
5.1	Participant Demographics Table	36
5.2	Device Sharing Privacy Concerns	59
5.3	Post-hoc S&P Strategies.	62
5.4	Digital Safety Teaching at Home	65
5.5	Participant Reported Design Needs.	72
6.1	Mapping of Device-Sharing Challenges to Needs	78

Chapter 1

Introduction

Nearly one in four Canadians is an immigrant, and a significant proportion of that population traces its origins to regions, like the Global South, widely characterized as “collectivist” [139]. Hofstede defines collectivist cultures as those in which individuals see themselves first and foremost as members of tightly knit social groups, prioritizing loyalty and relational obligations to that group over their own individual autonomy [76]. In their everyday life, these orientations manifest concretely in practices such as multi-generational living arrangements, pooled household resources, and collective, rather than individual, decision-making [129, 150]. Within these communities, device sharing follows naturally from this same orientation and is highly prevalent [8, 9]. To be clear, device sharing is not exclusive to collectivist households: it can also occur in non-collectivist households, where devices are lent, borrowed, or otherwise shared in situational and largely impromptu contexts [105, 98, 85, 79]. However, this situational sharing differs significantly from what occurs in collectivist households, both in how frequently it happens and in the factors that shape it [87, 9]: in collectivist households, devices are treated as communal assets from the outset, and access to them is negotiated on the basis of age, gender, purpose, and trust rather than individual ownership [9, 115]. Yet contemporary devices are built on the opposite assumption: most are designed for a single user, with authentication and access controls built around the expectation of just one signed-in individual [166, 28, 97]. Although some devices do offer separate profiles or guest modes as a partial accommodation [20, 114], these mechanisms remain fairly limited and unusable in practice and rarely accommodate the fuller social realities of collectivist households [8, 9, 115, 130].

These dynamics are further complicated once migration enters the picture. Prior literature describes how migrants remain embedded in values shaped by their countries of origin even as they simultaneously navigate the norms of their host society, producing an ongoing

blend of value systems rather than a clean replacement of one by the other [159, 102]. At the same time, life in WEIRD (Western, Educated, Industrialized, Rich, and Democratic) contexts like Canada, is increasingly mediated through digitized systems that touch nearly every aspect of daily life, from banking to schooling to healthcare, which correspondingly limits the extent to which families can simply opt out of them [163, 56, 159]. Caught between these two pressures, immigrant families must rapidly adapt to an unfamiliar digital infrastructure while still upholding the rituals of their home country. This tension is further heightened by the discrimination immigrant families frequently encounter and by the weak support networks they can typically draw on in a new country. Despite how much this tension effects their daily lives, it remains largely ignored in the literature [55, 30, 58, 133].

Furthermore, when families share devices, children face privacy risks that compound rather than simply add up: their browsing histories, messages, and social media activity become visible to other household members as a direct consequence of the shared setup, while their own risk-taking or naive behaviors online separately expose them to cyberbullying, hacking and fraud [169, 27, 99]. Because the device itself is shared, these risks do not stay contained to the child alone; they also put everyone else who shares that device at risk, so that virtually every consequence becomes a household problem rather than an individual one. Shared devices also complicate parental oversight. Parents typically attempt to mitigate these risks through monitoring and guidance [17, 162, 70, 62], yet these same protective measures often end up straining the parent-child relationship they are meant to protect [47, 14, 61, 168]. These dynamics are intensified further for immigrant families, specifically those who often have limited social and technical support networks to draw on within this new digital landscape [159, 148]. Despite all of these compounding factors, there remains only a limited understanding of how parent-child dynamics specifically shape privacy and security within immigrant families navigating shared-device environments [159].

We adopted a qualitative research design to address our research questions because the privacy and security experiences of Global South immigrant families in Canada remain largely unexplored in the existing literature. Semi-structured interviews were used specifically because they allow participants to describe their experiences, tensions, and underlying reasoning in their own words, rather than being constrained to a predetermined set of response categories. Beginning in September 2025, we conducted 41 semi-structured interviews with 19 parents and 22 children and young adults from 18 voluntary migrant¹ families, predominantly from South Asia, living in Canada, in order to answer our research questions.

¹Voluntary 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).

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 amplify 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 children use concealment to avoid parental surveillance, and how parents struggle to balance cultural preservation and 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 immigrant families face complex challenges 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 user 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.

1.1 Thesis Statement:

This thesis argues that shared-device use in collectivist immigrant households is a culturally inherited household practice shaped by migration, family expectations, and home country values. Drawing on interviews with immigrant families in Canada, it shows how shared phones, laptops, tablets, and accounts become sites of everyday family governance. These practices produce security and privacy risks that are shared across the household but experienced unevenly: parental protection towards children can become surveillance very quickly, and children's privacy tactics can introduce new security risks. Parents face responsibility and fragmented oversight, while children experience monitoring, loss of privacy, and constrained autonomy. By tracing how cultural expectations, family relationships, and migration shape shared-device use, this thesis argues that shared-device security and privacy must be considered as a default when designing digital devices.

1.2 Related Publications:

Significant portions of the research in this thesis have appeared in, or are based on, peer-reviewed academic work. I am the primary author of this work. Co-authors include her supervisors, Dr. Urs Hengartner and Dr. Leah Zhang-Kennedy, and Ameemah Humayun. A portion of the text from the published work is used throughout this thesis; however, this thesis is an expanded treatment of that research with substantial additional analysis and discussion, and no single chapter is drawn exclusively from the publication.

The peer-reviewed full paper publication is:

- **Shanza, S.**, Humayun, A., Hengartner, U., & Zhang-Kennedy, L. (2026). Sharing Digital Devices is Normal and Cultural: Privacy and Security Challenges in Collectivist Immigrant Households. *In Proceedings of the 2026 USENIX Symposium on Usable Privacy and Security (SOUPS)*, Hannover, Germany.

The poster publication is:

- **Shanza, S.** (2025). Toward Stronger Digital Privacy and Security: Culturally-Informed Solutions for Shared Device Use by Immigrant Families in Canada. Poster presented at the University of Waterloo Cybersecurity and Privacy Institute (CPI) Graduate Student Conference, Waterloo, ON, Canada.
(*Recipient of the Outstanding Interdisciplinary Poster Award.*)

1.3 Thesis Organization

The remainder of this thesis is organized to move from context to implications, each chapter building the foundation the next one needs. Readers looking only for the empirical findings can skip ahead to Chapter 5 (Findings).

Chapter 2 (Related Work): situates this study within existing research on migrant security and privacy and device sharing in collectivist contexts. It identifies the specific gaps that motivate this thesis: in particular, the limited attention that has been paid to how shared-device practices themselves travel with immigrant families into new sociocultural and digital environments, and how migration reshapes the risks those practices carry as well as how children, despite being highly vulnerable, remain largely under studied.

Chapter 3 (Methodology): describes the qualitative research design used in this study. It outlines the recruitment process, eligibility criteria, interview procedures, and participant demographics, and explains the approach taken to data analysis. Because this study involves interviewing multiple members of the same family about sensitive, sometimes conflict-laden household dynamics, this chapter also discusses researcher positionality the ethical considerations shaping the interview process, and the procedures used to handle participant data.

Chapter 4 (Limitations): discusses the boundaries of the study and in what context the findings should be interpreted. These include limitations related to recruitment channels, sample composition, language, the reliance on self-reported data, and the extent to which findings drawn from predominantly South Asian immigrant families in Canada may or may not transfer to other collectivist or immigrant contexts.

Chapter 5 (Findings): presents the empirical findings, organized around the study's three research questions. The chapter first examines how migration, cultural values, religious expectations, family authority, and intergenerational dynamics shape the way families share devices in the first place (RQ1). It then turns to the security, privacy, social, and moral risks that emerge once devices are shared, along with the strategies families use, often informally, to manage them (RQ2). Finally, it presents participants' own reflections on the limitations of their current devices and their suggestions for what would make sharing safer (RQ3).

Chapter 6 (Discussion): draws these findings together and connects them to broader implications for security and privacy design. It discusses how filial piety, religiosity, cultural expectations, and household governance jointly shape shared-device use, and why safety education in these households tends to emphasize avoidance of harm rather than a deeper understanding of it. The chapter then translates these findings into design directions for

devices to better support collective use rather than treating every user as an isolated individual.

Chapter 7 (Conclusion): concludes the thesis by summarizing the main contributions of the study and outlining directions for future research. It reflects on why shared-device security and privacy should be understood not only as an individual concern, but as a household-level issue.

1.4 Contributions:

This thesis makes four main contributions.

Documenting Shared-Device Use in Immigrant Families: First, this thesis documents an underexplored security and privacy context: shared-device use in collectivist immigrant families after migration. Through 41 interviews with 19 parents and 22 children and young adult dependents from 18 immigrant families in Canada, this work captures how device sharing is shaped by migration, cultural values, religious expectations, intergenerational relationships, and everyday household constraints. Rather than studying parents or children in isolation, this thesis examines both sides of the same family relationship, showing how the same shared device can represent protection and responsibility for parents, but surveillance, exposure, and restricted autonomy for dependents.

Identifying Device Sharing as a Mechanism of Family Governance: Second, this thesis shows that device sharing functions as a form of household governance. In the families studied, devices were not merely passed around for convenience or due to financial constraints. They were used to enforce rules, preserve cultural and religious values, monitor children’s behavior, manage fear in an unfamiliar digital environment, and maintain parental authority. Financial responsibility often became a justification for surveillance, while trust was unevenly distributed across age, gender, maturity, and perceived moral responsibility. This contribution moves beyond describing “sharing practices” and instead identifies the social mechanisms through which shared devices become instruments of care, control, conflict, and negotiation. And how trust moves along a spectrum from coercive to relational rather than sitting fixed at one point per family.

Reframing Security and Privacy Risks as Relational and Family-Wide: Third, this thesis identifies the household as the unit of security and privacy risk. Current security models often assume that a privacy breach or security failure affects a single user. The findings show that this assumption breaks down in shared-device households. Account mixing, saved credentials, visible notifications, algorithmic cross-contamination, unsafe downloads, scam exposure, and children’s risk-taking can create consequences for multiple family members at once. This thesis also shows that children’s heuristics for judging online risk: chiefly, treating familiarity as a proxy for safety, are shaped directly by growing up in a household that already normalizes handing access to anyone close. A child’s action may expose a parent’s financial information; a parent’s monitoring may expose family’s private life; and one person’s mistake can turn into a household-wide security event. This reframes shared-device risk as relational and cascading rather than individual and contained.

Translating Findings into Design Directions for Safer Shared-Device Use:

Fourth, this thesis translates participants’ lived challenges into concrete design directions for safer sharing. Rather than offering broad calls for “better privacy” or “more parental control,” this thesis identifies specific design needs grounded in the failures participants described: identity-aware profile switching, tiered visibility, app-level separation, household-scoped risk alerts, and cross-platform aggregation of parental controls. These directions aim to support shared use without forcing families into a false choice between total parental surveillance and total individual secrecy. These directions are not meant as fixed prescriptions, but as design starting points for recognizing shared devices as relational, negotiated, and culturally situated.

Chapter 2

Related Work

Understanding security and privacy in shared-device immigrant households requires drawing on two bodies of work that, until now, have largely developed in parallel. The first concerns how immigrants navigate security and privacy challenges more broadly, including the specific vulnerabilities introduced by displacement, unfamiliar institutions, and reduced social and technical support networks. The second concerns how device sharing itself operates in collectivist cultures, independent of migration, including how communal ownership norms interact with technologies that were largely designed around a single user. We do this because our participants sit at the intersection of both bodies of work, migrants who also share devices within collectivist family structures.

We organize this chapter into these two corresponding strands: (1) Security and Privacy challenges faced by migrants, and (2) device sharing in collectivist cultures and family dynamics that affect them. Reviewing them together makes clear what the existing literature lacks: it rarely considers what happens when both conditions hold at once, which is precisely the gap this thesis addresses.

2.1 Migrants and Security and Privacy Challenges

Migrants rely heavily on digital technologies to meet their everyday security, privacy, and transnational needs, using these tools not simply for convenience but to sustain the practical, financial, and relational demands of a life split across two countries [45]. Migration itself introduces an entirely new digital landscape, and this landscape is especially difficult to navigate for individuals coming from developing countries, because the risks it carries disproportionately affect marginalized groups: language barriers make everyday digital tasks harder to complete safely, and this unfamiliarity leaves migrants more heavily exposed to scams, surveillance, and fraud, a vulnerability that is further compounded by the discrimination and social isolation many continue to experience once they migrate [82, 83, 151, 55, 30, 58]. As a result, many migrants experience what has been termed as “*privacy turbulence*”: a persistent sense of uncertainty about how to manage their privacy appropriately, driven by not yet knowing the social norms, institutions, and expectations of their host country [143]. This general vulnerability is not distributed evenly across all migrants, however. Prior work documents the more specific digital vulnerabilities faced by particularly marginalized subgroups, including Muslim-American women and migrant domestic workers, both of whom report facing ongoing harassment and surveillance as a routine part of their digital lives [136]. For Muslim diasporic communities specifically, norms around modesty, gendered visibility, and moral accountability do not fade after migration; they continue to actively shape everyday digital practices, from what is shared online to who is permitted to see it [81, 113]. These expectations of modesty are not unique to Islamic contexts, either: similar norms recur across other religious traditions as well, including Hindu and Christian communities [49, 21], and in each of these contexts the same values that govern modesty offline are extended into digital spaces, meaning a violation online can carry reputational harm and a range of other social consequences just as a violation offline would [5, 130].

For immigrants who are additionally navigating shared-device and collectivist digital environments, these harms are often amplified well beyond what any individual would experience alone, because a privacy or security failure rarely stays contained to one person: it can rapidly escalate into a crisis for the entire household. Despite how serious this compounding effect can be, the literature has paid only limited attention to security and privacy issues among migrants as a population in their own right [133], to the concerns, attitudes, and behaviors of minoritized ethnic communities more broadly [126], and, more specifically still, to how the everyday practice of device sharing is itself shaped by the transnational cultural values that migrants carry with them. The research that does exist tends to concentrate heavily on U.S.-based populations, and even within the U.S. it

is largely confined to a handful of specific subgroups, such as international students, undocumented immigrants, refugees, and migrant domestic workers [148, 68, 167, 136, 156], while large-scale, representative work on voluntary migrants’ security experiences, specifically from collectivist cultures, remains scarce [73]. Even the smaller body of work that does focus on Asian immigrant populations compounds this narrowness further, tending to center almost exclusively on adult experiences and leaving families dynamics or young children within these same households understudied [159, 148].

This gap points to an opportunity to expand existing research beyond primarily individual-centered models of digital use, toward a fuller account of collective and relational household practices. Warford et al. argues that vulnerability in security and privacy research often arises less from any inherent trait of a population and more from users’ cultural contexts and the public roles they occupy, and propose a unifying framework for studying such “*at-risk*” populations. Treating migration status as one axis of structural vulnerability among several others, rather than as an isolated topic of its own [165]. This concern is echoed by work documenting an “*online privacy divide*,” which shows that privacy concerns and protective behaviors differ systematically across socioeconomic, demographic, and ethnic groups [101, 50], and by calls to move security and privacy scholarship beyond its traditional focus on privileged, Western populations toward the lived experiences of marginalized communities [137]. In direct response to this imbalance, researchers have increasingly called for “*inclusive privacy and security*” approaches that foreground the needs of under-served populations from the outset of system design [164], and for moving beyond a “*one size fits all*” model of the user toward research considerations tailored to the specific populations being studied [161]. Our focus on immigrant, collectivist, shared-device households follows directly from this line of argument: centering a population whose everyday practices sit outside the assumptions built into most security and privacy systems in digital devices.

Beyond the specific harms already discussed, migrants’ digital lives are also shaped by an ongoing, adaptive relationship with technology that existing research is only beginning to document. Recent work on educational migrants finds that their social media privacy practices evolve across distinct stages of migration, with users adopting increasingly segmented sharing strategies to manage separate audiences across home, diaspora, and host communities as they balance trust, cultural norms, and digital vulnerability over time [148]. This adaptive use is not incidental: digital platforms, and social media in particular, play an essential role in migrants’ lives by sustaining connections to home while simultaneously helping them adapt to new social and cultural environments [16, 149, 45]. Refugees and other newcomers in particular rely on mobile and online technologies to sustain transnational relationships and meet everyday integration needs [25, 45]. Migrants manage the resulting exposure through a mix of preventative strategies, such as deliberately limiting

what is visible to specific audiences, and corrective strategies applied only after a privacy incident has already occurred [93, 159]. Much of this literature, however, concentrates on economic migrants and refugees specifically, leaving voluntary migrants, such as the skilled-worker and family-sponsored immigrants in our own sample, comparatively under-explored, and it says relatively little about how these same adaptive strategies play out once a household, rather than an individual, is sharing the device those strategies are meant to protect.

To address these compounding gaps, this thesis examines how migration-related and sociocultural factors jointly shape the security and privacy challenges immigrant families face, paying particular attention to young dependents navigating these challenges within shared-device contexts. To do this directly, our interview protocol explicitly probed three things: migration-related changes in digital practices, privacy expectations shaped by culture, and security incidents participants encountered specifically after their move. Through this lens, we examine how migration reshapes existing device-sharing norms, produces risks that are specific to the immigrant household rather than to any single individual within it, and drives the adaptive practices families develop in response to those risks. Critically, by including parents, children, and young adults from the same household rather than sampling any one generation in isolation, we are able to capture within-family perspectives on the very same shared reality, allowing us to show concretely how security and privacy challenges unfold, and sometimes diverge, across generations and age groups within a single home.

2.2 Device-Sharing in Collectivist Cultures

Many communities around the world frequently share technology that is conventionally labeled as “personal,” treating devices as communal resources rather than individual possessions [105, 9], a pattern that directly challenges Western notions of “personal computing” as something inherently tied to a single owner [29, 153]. Matthews et al. offer one of the clearest accounts of what this sharing actually looks like in practice, classifying it into six distinct forms: borrowing, mutual use, setup assistance, helping, broadcasting, and accidental access [105]. This sharing extends across both physical devices themselves [142, 86, 41, 87, 90] and the accounts and credentials used to access them [51, 135, 89, 110, 117]. While this kind of sharing is not limited to any single part of the world, it is markedly more prevalent in collectivist and developing regions than elsewhere [142, 86, 111, 9]. Yet despite how common this sharing is, authentication and access-control mechanisms remain designed almost entirely around the assumption of a single, individual user [28, 153]. A study conducted in the U.S. shows that when people do share devices there, they manage this mismatch through careful, selective workarounds: they consciously grant access and adjust their authentication behavior on a case-by-case basis [123], and they retain strong expectations of individual control even over devices that are explicitly meant to be shared, such as household smart speakers [108, 2]. Collectivist settings present a striking contrast to this individually-oriented pattern: prior work shows that even devices as inherently personal as phones are routinely and openly shared among household members in these contexts [8]. In these settings, privacy is frequently treated as secondary to collectivist needs and obligations [130], and device sharing tends to be justified through narratives of care and tradition rather than through any language of surveillance or control [13], even though these same practices can simultaneously generate real tension and moral judgment within hierarchical family structures [14]. Further complicating matters, attempting to enforce strict, individually-oriented privacy controls within such households can itself strain relationships with family and friends, precisely because doing so runs against the shared, trust-based norms the household already operates by [8, 46].

Part of why single-user assumptions fail so strongly in these households is also technical, not merely social or cultural. Many personalization systems construct their behavioral models directly from activity tied to a single signed-in account or device, an architecture that breaks down as soon as multiple people use that same account or device. Incorporating several users’ actions into one model can produce inconsistent recommendations or unintentionally reveal one user’s private activity to another [154, 6]. This technical mismatch is compounded by a gap in how the phenomenon has been studied empirically. Much of the existing work on device and account sharing examines a single device or platform in

isolation, rather than capturing how sharing plays out across the multiple devices and accounts that coexist within one household, leaving only a limited, fragmented understanding of how sharing actually unfolds in practice [37, 43, 88]. This fragmentation is especially consequential in lower-income and developing-region contexts, where phone sharing is frequently the norm rather than a rare instance. Privacy has been described by participants as something other than an individual right in the first place [104]. Addressing this gap matters directly for design: without a more systemic, household-level view of sharing, it is difficult to build systems that reflect how sharing actually happens rather than how a single device or account is assumed to be used.

Ethnographic work in South Asia makes clear just how far this sharing extends beyond convenience. Field interviews with urban Indian families found that phone sharing was shaped as much by cultural norms as by economic constraint, with some married women reporting that they felt little need for a device of their own separate from their husband’s [141, 142]. Sharing of this kind is also easy to underestimate from the inside: users in a smartphone-sharing study consistently reported sharing their devices less often than their own logged behavior showed, suggesting that much of this sharing is treated as unavoidable background practice rather than a deliberate or memorable choice [69]. This same undercounting problem extends to children specifically. Large-scale European survey work finds that children commonly use household devices that are nominally their parents’, and that how a family manages this shared access depends heavily on household income, parental education, and parenting style, yet even in these comparatively well-resourced contexts the tools available to parents still inadequately support both effective parental oversight and children’s own privacy [100, 47]. This suggests that the mismatch between single-user device design and shared, negotiated household use is not confined to any one region or income level, even as its specific stakes, from reputational harm to religious boundary-keeping, are shaped by the cultural context in which sharing occurs.

The combination of this widespread sharing with the increasingly sensitive nature of the data stored on personal devices meaningfully heightens the risks families face, including misuse of shared access, moral judgment from family members, blackmail, account compromise, and outright data leakage [8, 9, 81, 87, 130, 15, 121]. These risks are not distributed evenly across a household, however. Broader social, cultural, and economic conditions [42, 120, 131], together with religious norms [3, 4], actively shape how these sharing practices unfold, and gendered norms in particular compound these dynamics further still, producing unequal access to devices and near-constant surveillance of women within these households [112, 80, 5]. Daughters in particular are often held to stricter limits on their mobility, social interactions, and online activity than their brothers. Restrictions that families typically justify through concerns about modesty, safety, and the reputational harm

that any perceived impropriety could bring to the family’s honor [112, 80, 67]. In response to these pressures, device sharing tends to prompt ad hoc, improvised protections rather than systematic ones [8]. Prior work on shared phone use among families in Bangladesh has suggested ways to separate shared and private content, such as a tiered privacy model that partitions accounts based on sensitivity [9]. However, it remains unclear how effectively such approaches would work in everyday shared-device contexts.

Because children are central actors within these shared-device ecosystems rather than peripheral to them [122, 162], the specific style of parental mediation a family adopts carries significant implications for both privacy and security outcomes. The evidence here points in a consistent direction: dialogue-based mediation, where parents talk through risks and expectations with their children directly, is associated with more positive outcomes overall [44, 162], whereas restrictive monitoring imposed without that same dialogue can actively undermine children’s technical and social digital skills rather than protect them [44, 99, 162]. Evidence drawn specifically from collectivist contexts adds further complexity to this picture, highlighting additional challenges such as risky teen behaviors and genuine difficulty achieving effective parental mediation amid rapidly rising device access among young people [128, 112]. Because this area remains comparatively under-researched, immigrant families are left largely unsupported as these same device-sharing challenges migrate with them into their host countries [159, 122].

To address these gaps, we interviewed parents and children together to examine how sociocultural values shape the governance of shared devices, and how families work to negotiate the tension between collectivist sharing norms and individual privacy needs. Our sample centers predominantly on first-generation South Asian immigrant families in Canada, offering a situated window into these dynamics within a community that remains specific in its cultural context yet meaningfully underrepresented in the broader literature. By capturing both perspectives of the parent-child dyad from within the same families, rather than sampling parents and children as unconnected individuals, our approach reveals relational tensions that single-sided studies inevitably miss, and that current security and privacy tools fail to support.

Chapter 3

Methodology

Throughout this thesis, the terms parent(s) and “dependent(s)” refer to participants’ relational role within the household rather than their legal age. Dependent participants include minor children (9–12), teens (13–17), and young adult dependents (18–25), reflecting their non-parental familial role. Where relevant to consent and assent procedures, we further distinguish younger children (9–12) from teens and young adults (13–25). Young adult dependents were included because many in migrant families from collectivist families still live with parents, also enabling insights into how device sharing dynamics change over age.

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. Gaming consoles were excluded from formal recruitment criteria but were occasionally discussed by participants where shared informally within the household. Across interviews, participants mostly spoke about devices collectively rather than individually or by type.

Figure 3.1 summarizes the overall study procedure. Eligible families were recruited and screened via a parent-completed survey, then took part in a single 90-minute session comprising consent, a brief demographic survey, and separate parent and child interviews. Sessions were followed by transcription and an iterative, cross-perspective thematic analysis process, described further below.

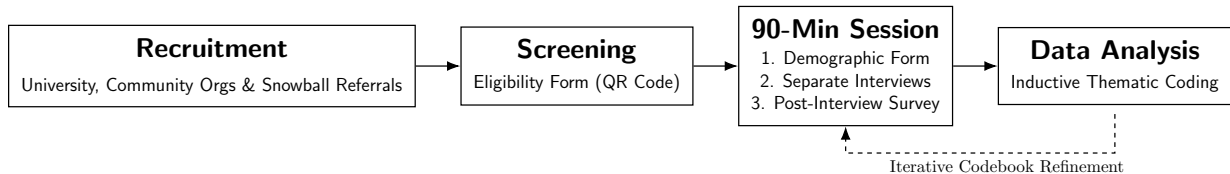


Figure 3.1: Overview of the Study Procedure.

3.1 Participant Recruitment

To ensure broad access to eligible immigrant families, recruitment combined university-affiliated and community-based channels. University-based recruitment included announcements distributed through university mailing lists, the Daily Bulletin, and the Weekly Newsletter. To reach families beyond university networks, we partnered with local community organizations serving newcomer and immigrant families, distributing materials through bulletin boards, email newsletters, and community mailing lists, and shared study invitations in Facebook and WhatsApp groups serving Global South immigrant communities, as well as recruitment flyers posted at grocery stores frequented by these communities. Snowball sampling was used sparingly, in two cases, to supplement outreach. All recruitment materials specified eligibility criteria, a brief study description, a QR code linking to the screening survey, and contact information for the research team and the University’s Research Ethics Office. The screening form given in Table 3.1 had to be completed by a parent and 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 [109]. We did not include non-immigrant families because prior literature already establishes baseline device sharing practices in Western contexts [15, 85, 87, 98, 105]. Instead, we report participants’ comparisons of pre- and post-migration experiences and their 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

Table 3.1: Screening Form Questions

No.	Question	Response Options / Details
1	Are you a first-generation immigrant in Canada?	Yes / No
2	How long have you lived in Canada?	Open response
3	What is your country of origin?	Open response
4	What languages are spoken in your home?	Open response
5	Do you live with your immediate family, i.e., spouse and children?	Yes / No
6	How many children aged 7–25 currently live in your household?	Open response
7	Please list the ages of the children living with you who are willing to participate in the study.	Open response
8	Do you or your family members share digital devices with one another?	Yes / No
9	Which of the following devices are regularly shared in your household?	Smartphone; laptop/desktop; tablet/iPad; gaming console, e.g., PlayStation; smart watch; e-reader
10	Why do you share these devices?	Financial reasons; convenience; safety and moderation for children; cultural norms; other
11	Would at least one parent and one child be willing to participate in a follow-up interview about device sharing at home?	Yes / No
12	Please provide your name and email address or phone number so we can contact you.	Contact information

as dependents if they lived with and shared devices with their parents. We targeted families originating from collectivist cultures, analyzed based on Hofstede’s individualism scale [76, 77].

We targeted families originating from Global South or collectivist cultural contexts, including South Asia (e.g., Pakistan, India, Bangladesh), Southeast Asia, Africa, the Middle East, and countries affected by conflict or displacement (e.g., Syria, Afghanistan, Iraq, Ukraine), as well as low- to upper-middle-income countries. Families who had lived in Canada for less than six months were excluded because they may not yet have established stable digital routines or adapted to the Canadian sociocultural environment, while those who had lived in Canada for more than twenty years were excluded to focus on families

still navigating dual cultural norms rather than those likely to be fully assimilated into mainstream Canadian digital practice. Participation was limited to individuals able to take part in English, Urdu, or Hindi, the languages supported by the interviewer, this ensured accurate comprehension of regional dialects and terminology.

Eligibility decisions were based on a holistic review of each screening response rather than a single criterion. We reviewed all screening forms and followed up with prospective participants. Among eligible respondents who responded to our interview invitation positively, participants were selected on a first response basis. Towards the last few interviews, we selected participants in a manner intended to support diversity across age groups, gender, and country of origin. All screening data were used solely for eligibility verification and were kept confidential. Eligibility relied in part on participant self-report; while this represents a trust-based approach, interview responses consistently aligned with stated eligibility criteria, providing post hoc confirmation.

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.

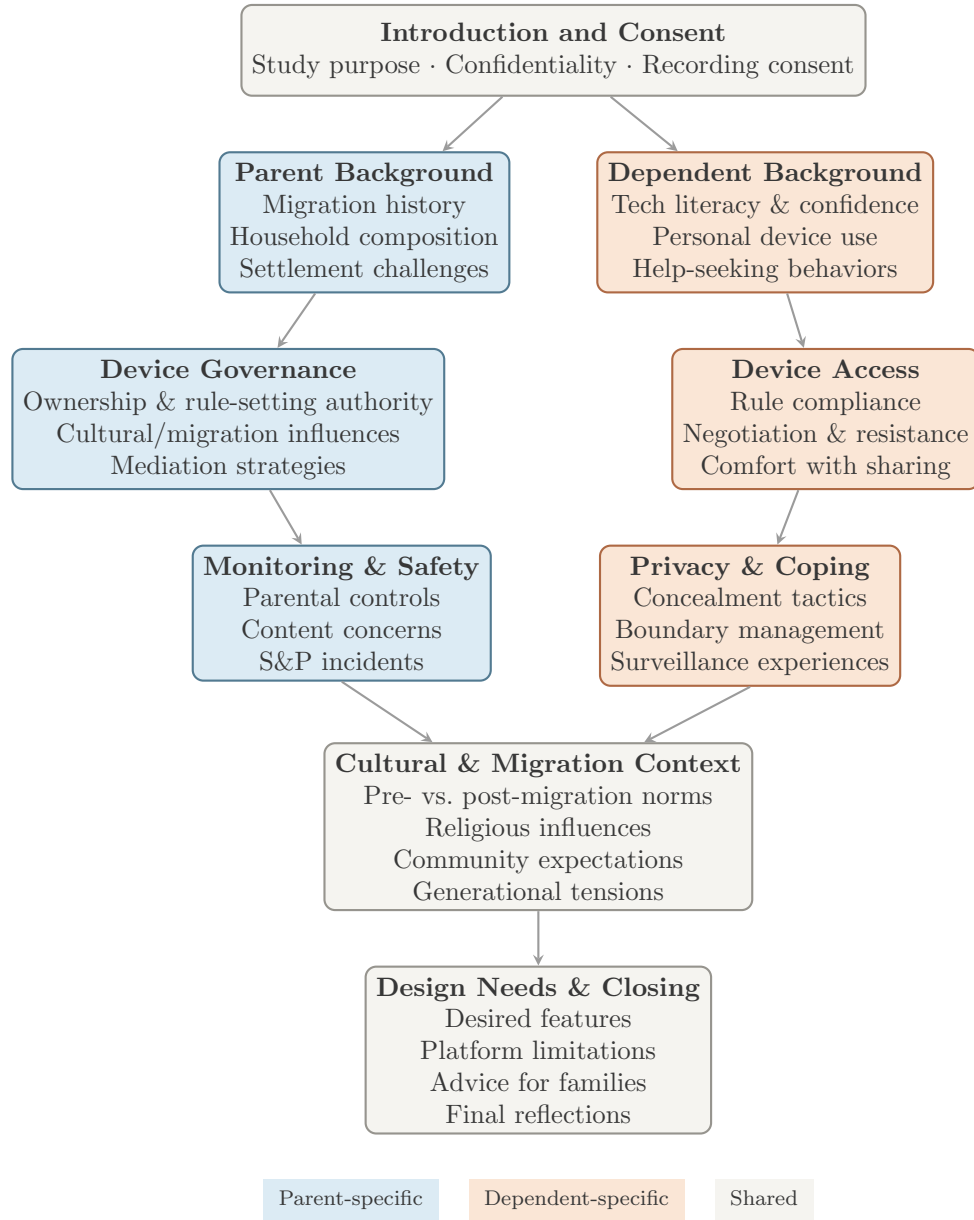


Figure 3.2: Semi-structured interview protocol with role-specific branches for Parents and dependents.

3.2 Interview Protocol

Each family interview session lasted approximately 90 minutes and mostly in-person, with about 20% being online due to participants' preference or distance. 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, security and privacy 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 security and privacy incidents, coping strategies, and desired design features. An overview of both protocols is included in Figure 3.2.

To minimize priming and social desirability bias, the study employed partial disclosure. During recruitment and consent, participants were told the study examined family technology use and shared-device practices; the study's specific focus on privacy and security was not emphasized at this stage, allowing participants to frame their experiences in their own terms. At the conclusion of each session, participants were fully debriefed: the interviewer disclosed the study's complete purpose, explained the rationale for partial disclosure, and addressed any questions or concerns. Participants were reminded that participation was voluntary and that they could request withdrawal of their data at any point during the session, or up to two weeks afterward. A written debriefing letter with follow-up contact information was provided to each participant. For in-person sessions, snacks and refreshments were offered as a gesture of appreciation for younger participants.

Given the sensitive nature of discussing family dynamics, privacy, and shared technology use, particular care was taken to build trust and rapport with participants, especially children. Interviewers introduced themselves as researchers rather than evaluators, explicitly framing the study as an opportunity to learn from participants' lived experience, with no right or wrong answers and no assessment of parenting quality, technical skill, or digital behavior. Participants were given the opportunity to ask questions before each interview began. Sessions opened with general, low-stakes questions about everyday device use before progressing gradually to privacy and security related topics, helping participants build comfort before engaging with more sensitive material. Interview rooms were arranged so that parents could visually observe their children without overhearing the interview, however none of the parents opted for invigilation, preserving both child com-

fort and response privacy. We used neutral, non-judgmental, age-appropriate language throughout, positioning participants as experts on their own experience, and introduced sensitive topics through hypothetical or anecdotal prompts rather than direct questioning. Participants were reminded they could skip questions, pause, or stop at any time without affecting compensation. To prevent cross-influence and protect confidentiality within families, interviewer did not share information between parent and child interviews. Given the sensitive nature of the study, this approach was judged to pose minimal additional risk.

Prior to the main study, we conducted a pilot study to validate the relevance of our research focus and inform the design of the primary study instruments. We conducted semi-structured interviews with six first-generation immigrant students who shared digital devices with family members. Transcripts were reviewed with particular attention to behavioral patterns and the role of cultural norms in shaping digital privacy practices. Several pilot participants independently raised privacy or security concerns arising from shared device use, reinforcing our motivation for the larger study. Insights from these interviews directly informed the design of the survey instruments and the semi-structured interview protocol described below. Pilot data were excluded from the final sample and analysis.

3.3 Data Analysis

Before the interviews, the participating parent completed a household demographics form. The form collected background information about the household, including migration history, education, employment, religion, languages spoken at home, household income, living arrangement, device ownership, device-sharing practices, digital rule-making, and access to private space. These responses were used to contextualize interview accounts and to describe the sample, rather than as the primary basis for analysis. The full demographics form is provided in Appendix B. Alongside that, all participants completed a brief survey including a modified version of the Security Behavior Intentions Scale (SeBIS), a security-knowledge test, and a self-confidence-in-security-knowledge scale, originally developed and validated by Kelley et al.[1]. Survey wording was adapted by age: participants 16 and under received a simplified, child-friendly version developed in consultation with a certified Canadian educator with 30 years of experience, while participants 17 and older completed the standard adult version.

Interviews were audio-recorded and transcribed using *Trint*¹, a GDPR-compliant service selected for its multilingual support and security protections. Transcripts were manually reviewed for accuracy and analyzed in *Atlas.ti*² using reflexive thematic analysis [38]. 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 complete interview guide is provided in Appendix A.

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 8 interviews, suggesting thematic saturation.

Coding was conducted at the family level, treating each family as a unit of analysis. Myself and A. Humayun independently coded the first six interviews using inductive open-coding [144], then met to resolve conflicts in our codes through discussion to develop the first codebook. I refined the codebook by applying it to four additional interviews

¹<https://trint.com/>

²<https://atlasti.com/>

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 [78]. A sample of the final codebook according to the RQs is provided in Tables 3.2, 3.3, and 3.4.

Following the interview, participants completed a brief post-interview questionnaire capturing device ownership, frequency of device and account sharing, relationship-specific comfort levels, and perceived privacy risks, the reason behind this was that there was some information which some participants, particularly children, found easier to report in a private, self-paced written format than verbally. Survey responses were analyzed alongside interview transcripts to further validate interview responses. Survey instruments complemented the qualitative interviews by capturing standardized measures of participants' security behaviors, security knowledge, and self-reported confidence, alongside structured reflections on device-sharing practices not always easily articulated verbally.

Table 3.2: Codebook Sample for RQ1

Code Category	Sub-Codes	Sub-Sub-Codes
RQ1: Sociocultural dynamics of device sharing		
Migration effects on	Home vs. Host Country	increased device dependence in canada; reduced supervision capacity;
Device-Sharing Norms	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	Promoting Religious Practice	device as reward for religion; religious content encouraged; fear of extremism
Cultural Transmission	Restricting Political Content	blocking politically content; propaganda in games / media
Conditional Ownership	Device Ownership as Conditional	independent device but supervised; cultural rules; religious rules
and Parental Authority	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	Reputation and Community Judgment	fear of host community judgment; extended family scrutiny
Screening	Compliance Framed as Morality	compliance is moral; privacy is a privilege; hiding is a guilt signal
	Moral Hygiene of Devices	“bad”; “clean” / digital hygiene ; install-delete cycles; self-censorship
	Romantic and Gendered Restrictions	dating prohibited; hiding romantic interactions; stricter rules for daughters
Power Imbalances and	Fathers as Primary Rule-Makers	father primary rule-maker; scared of father; rules for spouse
Gendered Control	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?”;

Table 3.3: Codebook Sample for RQ2

Code Category			Sub-Codes	Sub-Sub-Codes
RQ2: Security Landscape of Shared-Device Immigrant Households				
New Country, New Threats		New	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

Table 3.4: Codebook Sample for RQ3

Code Category	Sub-Codes		Sub-Sub-Codes
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;

3.4 Positionality Statement

The research team brings diverse cultural and migration backgrounds that informed both data collection and interpretation. A researcher’s background, experiences, and social position can shape methodological decisions as well as how qualitative data are interpreted. I conducted all of the interviews, being a recent first-generation immigrant from Pakistan currently living in Canada and having personal experience navigating shared-device practices, cultural norms, and privacy expectations within family settings. This positionality supported rapport-building and trust with participants, particularly when participants referred to cultural norms and practices implicitly. A. Humayun resides in Pakistan and also brings lived experience within collectivist Global South cultural contexts. U. Hengartner and L. Zhang-Kennedy are Canadian citizens; the former is a first-generation immigrant of European descent, and the latter is a Chinese-Canadian second-generation immigrant.

Myself and A. Humayun served as primary coders and brought lived experience with shared-device practices and collectivist cultural contexts, informing culturally grounded interpretations. At the same time, the research team remained attentive to the potential influence of insider assumptions. To mitigate bias, interpretations were discussed with the entire research team, allowing insider perspectives to be complemented by analytic distance. Reflexive memos were maintained throughout data collection and analysis to surface assumptions and document interpretive decisions. Collaborative analysis sessions supported cross-checking interpretations and ensured that themes remained grounded in participants’ accounts rather than researchers’ expectations. By combining cultural proximity with reflexive practices and team-based analysis, we aimed to balance contextual understanding with methodological rigor, strengthening the credibility and trustworthiness of our findings.

3.5 Ethical Considerations

Our study received approval from the University of Waterloo Research Ethics Board. We followed established ethical guidelines thoroughly to protect participant safety and confidentiality [31]. Participants were informed of their rights, including the voluntary nature of participation and their ability to withdraw their data up to two weeks following the session. Parents provided consent for their own participation and for their underage 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, due to 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 agency over how compensation is used or allocated.

To protect privacy, all data were anonymized using pseudonyms (e.g., M for mother and S for son). Personally identifiable information (PII), such as contact details, was stored separately from interview and survey data and used only for scheduling, compensation, and follow-up communication. PII was accessible only to myself. Research data were securely stored on University of Waterloo-approved, access-controlled platforms and will be retained for a minimum of seven years in accordance with institutional policy. Audio recordings were used solely for transcription and thematic analysis.

No ineligible participant data were retained, analyzed, or included in the study dataset. Screening forms were not linked to identifiable information beyond what was needed for initial contact, and ineligible individuals will not be re-contacted unless they had explicitly provided permission to be informed about future studies. This approach supported minimal data retention and protected the privacy of individuals who expressed interest in the study. All tools and platforms used in the study complied with institutional ethics and data protection requirements. Interviews were conducted using ethics-approved platforms, and only approved tools were used for data collection, storage, and transcription. Platforms not approved by the institution were not used for recording or storing participant data.

Participants were informed that their responses would not be shared with family members, and we avoid reporting intra-family identifiable references in our findings. We interviewed parents and dependents from the same household separately to reduce social desirability effects [72] and power dynamics [60]. 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.

Given the familial nature of the study and the use of snowball and community-based recruitment, particular care was taken to mitigate identity disclosure and de-anonymization risks. To reduce identity-disclosure risks, we anonymized all responses, balancing analytic transparency with participant safety. Relational metadata, such as explicit parent-child pairings, sibling relationships, or family group identifiers, were deliberately suppressed when reporting findings. Participant characteristics were reported in aggregate where possible, and certain demographic fields were omitted or coarsened to reduce the risk that participants could identify one another within shared social or community networks. 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 de-linked where needed. These decisions reflect a deliberate trade-off between analytic transparency and participant safety, prioritizing the protection of participants' privacy.

Participation in this study involved minimal risk. Some participants, particularly younger dependents, may have experienced mild and temporary emotional discomfort when reflecting on past experiences related to shared device use, such as conflicts with siblings, parental oversight of digital activities, or accidental exposure to personal content. Discussing household technology rules or privacy practices may also have evoked brief feelings of frustration, embarrassment, or self-consciousness, especially if participants perceived their practices as inadequate or unconventional. There was also a small risk of momentary social discomfort if parents and dependents became aware of differing perspectives on privacy, autonomy, or trust within the household. To mitigate this risk, interviews were conducted individually, and care was taken to ensure that participants did not hear each other's responses unless they explicitly chose to share together. No sensitive legal, medical, or traumatic topics were discussed, and the study did not involve deception, clinical intervention, or the collection of sensitive personal information beyond what was necessary for study logistics. Overall, any potential risks were expected to be mild, short-term, and non-lasting, such as temporary embarrassment or discomfort. No long-term psychological, social, or reputational harm was anticipated.

Chapter 4

Limitations

Participants were primarily recruited from a limited number of regions within Canada, and most families were located in mid- to large Canadian cities. As a result, our findings may under-represent families living in geographically remote areas, smaller towns or rural communities. Privacy practices, device-sharing norms, and access to community resources may vary across provinces in Canada. Although our findings offer insight into shared-device practices among immigrant families in Canada, they may not fully reflect the experiences of Global South immigrant families living in other geographic contexts. While our sample included participants from various countries of origin and religious backgrounds, it cannot capture the full range of collectivist immigrant family experiences.

While collectivist household dynamics serve as the broader conceptual lens for this work, the families in this study were predominantly first-generation South Asian immigrants. Findings should therefore be understood as reflective of this community and its specific migration, cultural, and family contexts, rather than as representative of all collectivist, immigrant, or Global South households. Families from other cultural backgrounds may organize privacy, autonomy, parental authority, and device sharing differently, especially where migration histories, religious practices, socioeconomic conditions, or technology access differ.

Recruitment relied on community organizations, social media groups, university networks, and limited snowball referrals. These channels may have favored families who were more socially connected, digitally engaged, or comfortable discussing technology-related topics. Families who are more isolated, less connected to community organizations, or less active on digital platforms may have been less likely to encounter or respond to recruitment materials. This may have shaped the sample toward participants who were relatively

willing to discuss household technology use and privacy practices. Recruitment through trusted community channels also helped reach families in a sensitive research context, but it may have introduced sampling bias.

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, digital rules, monitoring, privacy, or children’s autonomy. In some families, parents may hold different roles in technology management, discipline, religious guidance, or household decision-making. Interviewing one parent therefore limits our ability to compare parental perspectives within the same household. Future work could use paired approaches to better understand how parents negotiate digital rules and privacy expectations with each other, as well as with children. The interviewer’s language abilities and our recruitment channels may have introduced sampling bias, potentially excluding households whose primary language fell outside this range. Families who were not comfortable participating in English, Urdu and Hindi, the languages supported by the research team, may have been excluded. This is important because language access can shape both recruitment and participants ability to describe their experiences in detail.

As with qualitative work more broadly, our findings rely on self-reported accounts. Participants may not have remembered all device-sharing incidents accurately, especially when discussing past events, gradual changes after migration, or everyday household practices that had become routine. Their accounts may also have been influenced by social desirability, particularly when discussing parenting practices, children’s online activities, family conflict, religious expectations, or privacy violations. Although interviews were conducted separately and rapport-building strategies were used to reduce judgment, participants may still have selectively emphasized certain experiences or underreported others. This limitation is especially relevant in family-based research, where participants may be cautious about disclosing information that could reflect negatively on themselves or other household members.

Finally, this study prioritizes depth over breadth. It develops a detailed account of how shared-device practices intersect with migration, culture, family relationships, privacy, and security in everyday life. The findings reveal recurring patterns across the participating families while also showing that these practices vary according to family structure, cultural and religious expectations, socioeconomic circumstances, digital access, and relationships between parents and dependents. Future research can build on these findings by examining how such patterns appear across a wider range of immigrant communities.

Chapter 5

Findings

This section presents the findings of our study in three sections: (RQ1) First, we discuss device sharing practices in immigrant families and the influence of sociocultural factors on these practices; (RQ2) then, we explore the Security and Privacy challenges that arise during device sharing and the mitigation strategies these families adopt; (RQ3) and lastly, we report participants' perceptions of how effectively current devices support sharing and their recommendations for making devices safer for sharing.

Occurrence of a Theme: To help readers gauge how widely particular themes appeared across interviews, we provide approximate prevalence ranges following prior qualitative studies of the same nature [134, 53, 172]. Throughout this thesis we use the following descriptors with indicative ranges, applied to the relevant participant group (parents or dependents) as shown in Figure 5.1.

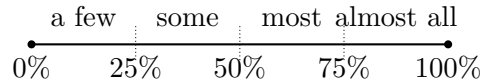


Figure 5.1: Terminology Used to Present Relative frequency.

Participant Notation: Participants are identified with a unique ID (1-41) prefixed by their familial role: M (Mother), F (Father), S (Son), D (Daughter). For example, F3 denotes Father with unique ID #3 and D26 denotes Daughter with the unique ID #26. To reduce the risk of identifying individuals within families, we did not link participants' familial relationships in the findings.

Participant Demographics: Table 5.1 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 (only five families included three participants). The average number of people per family that shared devices was three. Participants’ ages ranged from 9 to 57 years. Parents ranged from 34 to 57 years of age (mean = 42.9, median = 42), while dependents ranged from 9 to 25, spanning school-aged children, teens, and young adults living at parent’s home. The sample included 26 female participants, 15 male participants, and no participants who self-described as any other gender. Households varied in size from 3 to 7 members (mean = 4.37) and included nuclear and extended-family living arrangements. A full breakdown by role, religion, country of origin, occupation, education, age, household income, and years in Canada is provided in Table 5.1.

While household income was recorded as part of the demographic survey, socioeconomic context also emerged repeatedly within the qualitative data itself, mainly through participants’ discussions of financial constraints, shared household resources, and reliance on family plans or shared accounts. These qualitative accounts enrich the quantitative income bands by showing how financial considerations shaped participants’ motivations for device and account sharing, beyond what a single income bracket can convey.

Through the survey we found that despite comparatively strong self-reported security behaviours e.g., locking devices, checking links before clicking, all participants reported substantial uncertainty on basic security-knowledge items: 50% of participants aged 16 and under and 59% of participants aged 17 and older answered “I don’t know” when asked whether an IP address can reveal where they live, and 57% and 26% respectively answered “I don’t know” when asked whether public Wi-Fi is safe for sending private information. Practiced habits, in other words, are not accompanied by a commensurate understanding of why those habits matter, in either generation.

Adults reported strong, consistent engagement with basic, system-enforced protections, such as using a passcode to unlock their phone ($M = 4.78$) or a password on a laptop or tablet ($M = 4.41$), but weak engagement with practices that require ongoing effort or judgement, such as proactively changing a password ($M = 2.22$) or strengthening it beyond a site’s minimum requirement ($M = 2.78$). Children and younger dependents showed a related but distinct pattern: moderate engagement with basic device-locking behaviours ($M = 3.33$ – 3.60) and comparably weak password-hygiene practices ($M = 1.67$ – 2.67), but the strongest scores of any group on reactive, awareness-based behaviours, checking whether a link looked safe before clicking ($M = 3.73$) and telling an adult about something unsafe rather than ignoring it ($M = 4.07$). Both age groups default to whatever protection the device enforces automatically, under-engage with practices that require sustained effort, and, in children’s case, respond to visible danger without acting to prevent it in advance.

Table 5.1: 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	1
						Eritrea	1
						Zimbabwe	1
						Afghanistan	1
						Palestine	1
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

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 5.1). 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.

Households reported an average of 4.37 members but most had only two to three bedrooms, and just 42% of parents reported having access to a fully private room of their own ($n = 19$). Devices themselves were unevenly distributed relative to people: households owned an average of 3.21 smartphones and 2.63 laptops, and how much sharing occurred depended on device type, with laptops and desktops shared in 89% of households, smartphones in 67%, and tablets in 61% ($n = 18$). Sharing was also governed rather than incidental: 79% of parents reported that their children were expected to ask permission before using a parent’s device, a norm that was not reciprocal. Shared physical space and shared devices were compounding, not independent, conditions, and access to a shared device was something to be requested rather than simply taken.

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). And how can we better design devices for safer sharing (Section 5.3).

Conceptual Overview: Figure 5.2 provides a conceptual overview of the study’s findings. It shows how post-migration conditions and collectivist household norms shape shared-device practices in immigrant households, including the ways parents attempt to govern device use through moral, religious, financial, and fear-based forms of control. Because commercial devices provide weak support for multi-user family sharing, with limited role-based separation and frequent mixing of accounts, notifications, and recommendations, these governance practices produce a shared but unequal landscape of risk. Parents face responsibility, emotional strain, and fragmented oversight, while children experience surveillance, privacy loss, self-censorship, and constrained autonomy. Both groups respond

through reactive and improvised coping strategies rather than through reliable systemic protections. Taken together, these dynamics reveal two broader structural tensions: the mismatch between single-user device design and collectivist shared-device realities, as well as the tendency of users to equate safety with diminished privacy. These tensions motivate the design directions proposed in this thesis. Particularly the need for shared-device systems that support role-sensitive access, flexible visibility, and privacy-preserving forms of parental assurance. Rather than prescribing fixed technical solutions, these directions point toward design possibilities that better recognize shared devices as relational, negotiated, and culturally situated spaces.

Shared-Device S&P Landscape in Collectivist Immigrant Households

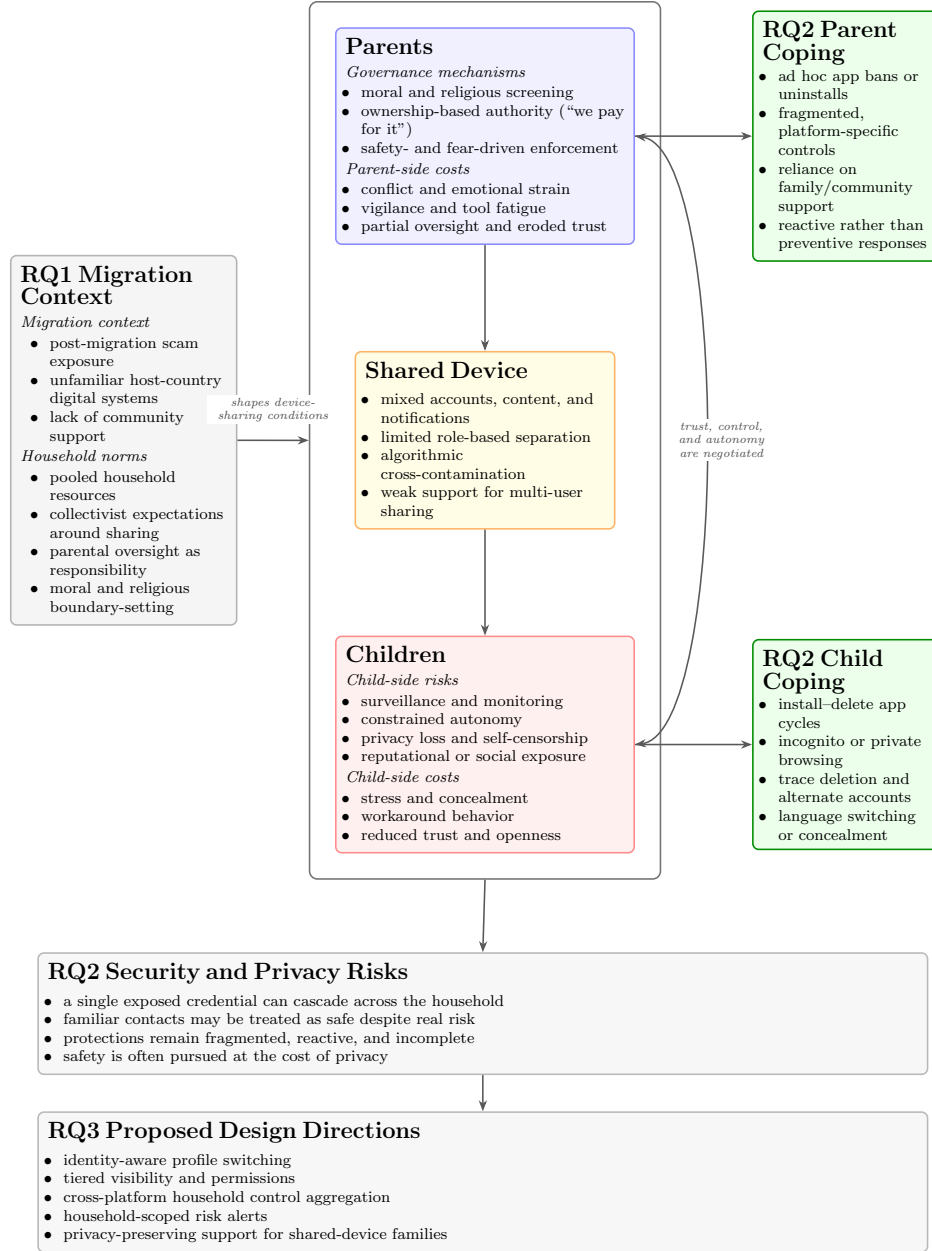


Figure 5.2: Migration and cultural context shape device-sharing norms and parental governance practices (RQ1). These practices generate distinct but interconnected risks and coping strategies for parents and children (RQ2). These tensions motivate the design directions proposed in this thesis (RQ3).

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 for dependents due to closer supervision, denser social networks, and more structured routines, reducing both device provision to dependents and hence, 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 to dependents and increased reliance on device sharing as a compensatory monitoring strategy by parents. 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 device 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, parents’ monitoring capacity, and migration-related concerns such as device sharing being a moral safeguard against complete device autonomy. 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”* (M17,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 strategy. 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

Section 5.1.1 establishes that migration reduced parental oversight capacity and increased reliance on shared devices as compensation. Underneath that shift sits a more specific structural cause: in participants' home countries, supervision was distributed across a household of people most joint family structures typical to collectivist cultures, while in Canada it collapses onto one or two working parents, and devices are used to fill the resulting gap.

Several parents described this collapse explicitly. One father, asked why managing children's digital lives felt harder in Canada than it had back home, located the difference in household composition rather than culture or technology: *"I guess back home we... we're not as much isolated as we are here. We live in a big family, there's so many members in the family to keep you busy, to keep your child busy. Or to watch them... Like over in here in Canada if you don't have your grandparents or your parents living with you, it's difficult for a parent. Like especially in cases like me and my spouse. I work days and he works evenings. So it's only one parent at a time in the house"* (M12). This account reframes early device provision not simply as a reaction to unstructured time, but as a direct substitute for the supervisory labor that grandparents, aunts, uncles, and older cousins would otherwise have absorbed.

A second parent made the same point about a different domain, modesty and self-presentation, describing how the disappearance of a wider household changed not just *how much* supervision was available, but *where* a child's moral education came from at all: *"kids were learning the same things at school. They were... learning through your grandparents, your other family members, your teachers, your schools, your other relatives. But here it's just us, and us against the world, I feel"* (M10). This "us against the world" mindset is a distinct migration effect: it is not only that parents have less time, but that the *family structure* transmitting cultural and safety norms to a child drops sharply after migration, and shared devices, through monitoring, content curation, and religious-app provisioning (discussed further in this section), become one of the few remaining mechanisms for reproducing a form of oversight and upbringing that used to be ambient rather than deliberate.

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 dependents’ risky digital 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 chose 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, while 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 of the family (M12). Romantic or cross-gender interactions were often prohibited across different age groups, and dependents reported concealing such activity to avoid conflict with parents. Across households with Muslim, Sikh, and Christian backgrounds, shared-device access functioned as a central mechanism for monitoring and constraining social ties and online self-presentation. Some parents extended this vetting beyond the peer to the peer’s family, treating shared religious or parenting values as a precondition for approved contact: *“We make sure that the kind of friends she makes, and the families we interact with, are also on the same page when it comes to parenting... religion derives a lot of values in my life”* (M10). 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 “It’s Yours, But Not Really”

Even when dependents described a device as belonging to them personally, ownership rarely functioned as an unconditional right. Dependents instead described access to “their” devices as continuously supervised, scoped to a specific purpose, and revocable at a parent’s discretion. In several families, a device assigned to a child came with an explicit purpose restriction rather than open-ended use. As one father explained of his children’s laptops, “*They are their device, but they can’t use them whenever they want... I keep the control of it. Kind of their device, they do their school work on it*” (M12). Assigning a device to a particular child indicated who it was for, not who ultimately controlled how and when it could be used. Dependents themselves frequently described acquiring a device as the outcome of active, ongoing negotiation rather than something owed to them. One daughter recalled preparing a formal presentation to convince her father to let her have a phone years before he considered her ready: “*I even made a whole document, a slide[deck] and all that... just to convince him. My dad was still not convinced*” (D20). Even after her mother intervened on her behalf and her father relented, permission remained conditional rather than settled with a warning that if she misbehaved or misused the phone, they would take it back. What began as a negotiated concession continued to carry the possibility of reversal indefinitely, regardless of how long she had had the device.

“We Pay For It”: Financial responsibility was one of the most consistently invoked justifications for parental authority over shared devices, raised independently by both parents and children. Because parents had purchased the devices and paid for the subscriptions and data plans attached to them, both generations tended to treat that financial responsibility as conferring a corresponding entitlement to full visibility and control over access and monitoring. Variants of “we pay for it” and “they pay for it” recurred in close to verbatim form across a wide range of otherwise distinct households, making this one of the most widely and consistently reported justifications for surveillance across both parents and children in our dataset. Financial responsibility functioned as a largely uncontested, culturally legible basis for control.

5.1.5 Gendered, Spousal and Power Dynamics

Device governance in several households was not distributed evenly between parents but mostly concentrated in one parent, typically the father, as the primary rule-maker, with monitoring tools and restrictions configured and enforced unilaterally. One mother described living under filters her husband had set for children, that were strict enough to block her own work- and school-related browsing, not only her children's: content controls intended for the dependents extended, by virtue of shared-device architecture, to constrain the supervising parent as well. Rather than contesting these restrictions directly, some mother-daughter pairs described a quiet camaraderie that formed around jointly concealing activity from the father, suggesting that gendered power imbalances in device governance can produce lateral alliances among those being governed, rather than only vertical conflict between parent and child.

Our data also contains a distinct version of gender asymmetry: parents' own childhoods, and the differential freedom they were given as sons or daughters, resurfacing directly in the rules they set for their own children now. One dependent traced this continuity across three generations in a single account, contrasting her father's adolescence with her mother's: *"my dad, obviously he's a boy, so he had it differently no matter what... my mom, she was always telling me how she was that girl that got really good grades, but she also kind of had fun... her dad didn't let her go to a lot of parties"*, while her father, by contrast, *"was allowed because he was a boy"* (D20). She connected this directly to her own present-day frustration, describing the resulting rules as a hand-me-down asymmetry rather than a reasoned response to her: *"it's always been so unfair to me... my dad didn't get his first phone until he was eighteen. So it's always been so unfair"* (D20), the double standard her parents grew up inside becoming, in her account, the felt injustice of her own household rules, even though her parents' stated reasoning was safety rather than gender as such.

A parent's account shows the other half of this mechanism: gendered risk perception shaping differential monitoring intensity between siblings. When asked how comfortable she felt about each of her three children using a shared device, one mother described a clear gradient tied partly to birth order but explicitly to gender for her middle child: *"with the second one, the boy, I'm a bit concerned... he tends to play a lot of online games, and I'm sometimes worried... that he's not playing violent games"* (M18), a level of specific, gender-inflected concern she did not extend to her elder daughter, whom she described as already having *"proven to be responsible."* These accounts suggest that gendered rule-setting in these households is an inherited pattern, carried forward from the parent's own adolescence and reactivated, sometimes unconsciously, on their own children.

Fear as a Mechanism of Governance: *"When they don't feel fear, they don't stop*

doing things” (M10). In several households, parents relied less on formal digital tools for device-sharing governance than on high-intensity emotional strategies, such as yelling, anger, and the deliberate induction of fear, to enforce compliance. Parents also explicitly linked these strategies to familiar norms from their countries of origin: *“I can control things through the app, but we usually don’t do that. Because of our ethnicity, like the region we come from, we end up having to shout at the kids and say, ‘Okay, stop it now.’ That eventually works, and nothing else really does”* (F5). Noncompliance was sometimes framed as an added burden on an already strained life, which some parents invoked to justify escalation: *“I do get angry... I do sometimes scream at them... Don’t add more things to [my problems]”* (M12). For children, refusal was rarely treated as a viable option: resistance was met with overwhelming emotional force on both sides. One parent described a child’s reaction to being denied a device: *“If they deny me... I’m gonna take the device and I’m gonna lose my mind”* (M12). Another parent reported an escalation that became physical toward the device itself: *“My wife broke his laptop”* (F1).

5.1.6 Surveillance, Conflict, and Emotional Strain

Monitoring was a major source of conflict in our sample. Parents framed checks as non-negotiable protection, while children experienced them as violations they had no real ability to contest. As one child explained, *“My parents used to take my phone and go through social media, and if they didn’t approve of something, we would fight about it. This happened a lot”* (D25), a pattern one mother also acknowledged from her own side: *“Sometimes they fight... ‘Why you chat with this person, why you talk like this, why you use this phone’”* (M11). Children described device governance as emotionally taxing in itself, marked by persistent anxiety under surveillance rather than by any actual wrongdoing: *“You’re constantly anxious or stressed even though there is nothing going on”* (D27). Several reported feeling “too scared” to hand over their phone (D26) or “paranoid if they’re going through my messages” (S40).

Disclosure to parents was often perceived as risky rather than supportive. Children described these conversations as “traps” that led to punishment instead of understanding: *“I feel like telling your parents something is always a trap, they act like they’re your friend or something, but then if it’s like something bad then they start yelling at you”* (D20). Others described feeling dismissed or embarrassed when privacy requests were ignored, or when their searches were read aloud: *“Sometimes they yell out what I search, it makes me feel a little mad and embarrassed”* (D30). In the absence of a trusted outlet within the family, children often withdrew and sought alternate ways of processing frustrations they could not directly confront: *“I’ll start writing in my diary”* (D27), and *“I’ve been asking*

for like a therapist ‘cause I just like talking about things that I’m not comfortable telling ‘em...” (D20).

Siblings as Informal Monitors: Beyond the parent-child relationship, several children identified siblings as a distinct source of surveillance risk within the home. Because siblings often shared the same devices and social circles, they were uniquely positioned to discover, and at times exploit, information a sibling would have preferred to keep private. One participant described this directly: *“My brother told my mom that I have a boyfriend on Snapchat, which I don’t”* (D26), while another described siblings using such knowledge as leverage: *“When they [siblings] blackmail me, like, ‘Oh, I know your secret, I’m gonna tell mama or I’m gonna tell papa’”* (D26). For several children, the most consequential privacy threat inside a shared-device household came less from external actors such as hackers than from these in-home dynamics: ongoing fear of a sibling’s disclosure, escalating parental monitoring, and reputational damage if peers or relatives discovered something kept private. We found that sibling relationships account as a distinct risk vector in shared device households.

5.1.7 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 as 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.

5.1.8 Trust as a Spectrum: From Coercion to Connection

Trust emerged as a central organizing concept in how immigrant families negotiated device sharing, not as a binary state that families either possessed or lacked, but as a spectrum shaped by adaptation to Canadian norms, parents’ perceived loss of authority following migration, and each family’s tolerance for divergence between parents’ and children’s values.

Conditional Trust: At the coercive end of the spectrum, trust functioned as a rule rather than as a relationship. Parents declared trust in their children while simultaneously expecting guilt- and responsibility-driven compliance, and maintained strict surveillance regardless of that stated trust: *“We have told her that we trust you... and if you hide something that means it is wrong. So she’s careful because of this”* (F2). Children experienced this framing less as genuine trust than as a moral obligation imposed on them: *“They will say, ‘Oh, we trusted you with this and that and I betrayed them’”* (D26). Within these households, parental authority was treated as effectively absolute: *“In my culture... whatever your parents say it’s final”* (D21).

In slightly less restrictive households, trust operated more like probation than a settled judgment about a child’s reliability, and was often shaped by practical constraints on a parent’s capacity for oversight rather than by trust itself: *“We cannot take it away completely... but I cannot enforce it because of my busyness... so there is like [a] dilemma, [a] trade-off existing”* (F1).

Relational Trust: Further along the spectrum, some parents had moved toward more trust-based approaches after recognizing that strict control risked damaging the parent-child relationship itself: *“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). In these households, parents described deliberately moderating their own reactions in order to preserve their children’s trust and willingness to disclose: “*She was scared a little bit... I did not react because I’m scared that then they will stop telling me all these things*” (M12). Even so, this relational trust often coexisted with a degree of strategic ignorance, in which parents preserved the relationship by deliberately not seeking out information that might conflict with their own values: “*I don’t want to know what they’re doing*” (M16). At the most relational end of the spectrum, parents and children described a genuine alignment of values, whether because children had become “*more Canadian*” in outlook, or because the family remained deeply collectivist in ways both generations endorsed. Both described trust in explicitly normative terms, as definitional to family membership itself: that “family means trust,” and that there should be “***nothing to hide from family.***”

The post-interview survey supports this reading numerically. Parents reported similarly high mean agreement (5-point scale, $n = 18\text{--}19$) with both trust-language items: “*I trust my child to use my device responsibly*” ($M = 3.95$) and “*I trust my child to respect my device and not access things without permission*” ($M = 3.84$); and monitoring-endorsement items: “*I believe it’s okay to monitor my child’s device when needed, it’s part of being a family*” ($M = 3.79$) and “*I believe parents have the right to access their child’s device when needed*” ($M = 3.74$). A small number of families described a pattern that sits outside this negotiated spectrum entirely: an explicitly open-trust model in which all household members comfortably accessed one another’s data as a matter of course, with no ongoing negotiation of boundaries. As one father described it, “*all of our family members can see everything of each other,*” adding that this arrangement “*never ended with an argument or fight*” (F7). Unlike the relational trust position above, where alignment is reached through negotiation or adaptation over time, this pattern treated mutual visibility as the default condition of family membership from the outset, rather than an endpoint reached through repair. These accounts suggest that the coercive, probationary, and relational positions on this spectrum are not fixed family traits, but points families can move between over time, often in direct response to specific ruptures or repairs in the parent-child relationship. Hence, tools built around an assumption of relational trust, may be poorly suited to, or even actively resisted within, households still operating under more coercive or probationary dynamics, and vice versa.

5.1.9 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,” of devices, keeping shared devices free from material deemed socially, culturally or religiously 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 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 other parents 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 by parents.

Shared Devices as a Marker of Good Parenting and Good Children: a few participants comparing their household to peer households concluded that children who share devices turn out better behaved and higher-achieving than children who do not. One dependent offered this comparison in direct response to a question about how his family’s rules differed from his friends’: *“a lot of them just have their own everything, their own laptop, their own console, their parents don’t check their phone, they won’t check anything... but usually what I saw is the kids who do have their own everything are just less well-behaved. Maybe they do less well in school... even some of my friends [who] share phones, those ones are usually the best in school and most well-behaved”* (S37).

A second participant, comparing the same contrast from the opposite direction, characterized peers with fully independent, unmonitored devices in stronger terms, not simply less well-behaved, but ungoverned: *“my friends get like complete anarchy, they get into*

whatever they want, whenever they want, and their parents don't really know what they're doing... their parents are more like, you'll figure it out if you go, rather than checking what you're doing to make sure you're going on the right path" (S35). The phrase "the right path" recasts device monitoring not as restriction but as a positive identity and reputational resource.

From External Rule to Internal Compass: Several older dependents describe a point at which externally enforced rules stop requiring enforcement at all, because the reasoning behind them has been internalized independently of ongoing parental monitoring. One young adult described this shift as complete and largely permanent, distinguishing it clearly from mere habit or fear of being caught: *"it's not like something you're reminded of every day... they've taught us why it's prohibited... and why it is wrong. So that's just embedded deep into my brain and my knowing. So they don't even have to tell me anymore because they've taught me why it's wrong. It's in my head, I just know to stay away from them"* (S40). The same participant, describing an earlier incident in which his mother discovered him texting a girl, located the moment of internalization precisely: rather than imposing a new restriction, she explained her reasoning once, and no rule was needed afterward, *"she just explained to me why it was bad, I think I knew in my head what to do"* (S40). Notably, no monitoring or restriction followed; the explanation itself was the entire intervention.

This same participant also described the underlying cultural logic he had to reconcile: an inherited expectation of unquestioning deference, *"you don't say no to your elders"*, set against a Western model he had partially absorbed since migrating, concluding that he now operates as a mix of both rather than a resolution of one into the other: *"in certain aspects we're more Western and in other aspects we're more... desi[cultural]"* (S40). This matters for the trust-spectrum argument in 5.1.8 because it clarifies what lies *past* the relational end of that spectrum: not simply a family that has agreed to trust each other, but individuals who have internalized the household's moral logic to the point that external enforcement becomes redundant.

5.2 (RQ2) Shared-Device Security and Privacy 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. Figure 5.3 summarizes these challenges.

5.2.1 New Country, New Threats

A few participants reported heightened Security and Privacy concerns after migrating to Canada, consistent with prior work on collectivist groups' and immigrants' scam vulnerability [82, 83, 151, 71, 73]. 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 commuters' 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. Another participant noted that these threats were uncommon in their country of origin (F3), aligning with evidence [151] indicating that Canada faces a disproportionately high share of fraud-related spam calls, suggesting that residents may face more aggressive scam targeting than their American counterparts.

5.2.2 One Device, Too Many Users

Almost all participants mentioned how shared devices created distinct Security and Privacy 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. Two incidents explain the set of safety-critical exposures on shared devices. A teenager described being startled to see his parents kissing on a shared device (S40), and one mother recounted her child encountering unexpected sexual content through an advertisement: *“a screen popped up full of nudity... that’s when I realized how dangerous it is”* (M10). Both incidents reinforce that exposure to inappropriate content on shared devices was rarely the result of a child’s own search behavior, but instead arose passively through the ordinary use of a device several family members relied on for unrelated purposes.

A few families also reported *“algorithmic mixing”* where one person’s activity reshaped content and ads for others on the same device. This contamination extended beyond content recommendations into how parents interpreted the device itself: several described the resulting stream of hyper-targeted ads as a form of surveillance in its own right, with one parent noting how quickly a single search translated into content elsewhere on the device: *“Literally, 5–10 minutes later we got a reel...”* (F2). Algorithmic mixing was also described as a source of risk rather than mere annoyance, at times surfacing content a parent would not otherwise have encountered, including advertisements for concealment tools: *“I found an app... basically erases all context of the thing... I just found it on YouTube... there was an ad”* (D20). Parents felt they had little recourse once a platform began amplifying a piece of content a child had engaged with: *“Those are things we can’t control. And we can’t sit on their heads either”* (M17). Some also noted that this exposure was uneven across device types, with algorithmic mixing felt more acutely on phones than on computers, where separate operating-system profiles offered at least partial insulation: *“the algorithm will not be impacted. These things exist on computers, but not on phones”* (F2).

Several families’ security practices revealed that a single shared or interconnected account, most often email, functioned as a structural single point of failure across the household. Much of this confusion traced back to a structural cause rather than individual carelessness: households rarely maintained role-based account separation, relying instead on shared logins and default profiles that made one person’s activity indistinguishable from another’s. As one parent put it plainly, *“on phones, we don’t really have separate profiles”* (F2), while a dependent described simply using whichever account was already open: *“I don’t have my own account... whichever one they pick”* (S34).

Others reported that even where separate accounts existed in principle, they were rarely maintained in practice: *“the Gmail accounts stay open. . . we don’t really care”* (D33). This lack of separation meant that a single mistake, once made, was rarely contained to the person who made it. Because shared accounts frequently doubled as gateways to banking, work, and other identity-linked services, one exposed credential could cascade well beyond its original context: *“Email is connected to everything. . . if he accesses that, everything else is open”* (F1). Passive exposure compounded this risk further, as message previews and notifications routinely surfaced private content without any deliberate act of surveillance: *“My dad gets notifications of my Gmail. . . then he calls my mom and tells her what I’m talking about”* (D26). Taken together, these accounts suggest that shared-device security in these households depends less on any single weak password or careless click than on an underlying account architecture in which one shared credential can cascade into exposure across nearly every domain of family life.

Across families, parental knowledge of children’s passwords was common, often framed as necessary for supervision, safety, or account management. Many parents described knowing their child’s password, creating passwords on their behalf, or logging in for the child rather than sharing credentials directly. In some cases, children’s devices were reported to have no passwords at all, or relied on biometric access such as Face ID, which parents could bypass or control. In scenarios where children had personal passwords, they could not refuse to disclose them when parents demanded it. In immigrant households, financial constraints and cultural expectations sustained device sharing and intensified its vulnerabilities. With fewer devices to go around and stronger normative expectations of pooled family resources, the same account or device was routinely stretched across roles it was never designed to separate, turning ordinary mix-ups into recurring, and at times high-stakes, points of family conflict. Some parents asserted authority by uninstalling apps, particularly games and social platforms.

While Kumar et al. [92] 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 more pragmatically, limiting their own use and deliberately keeping *“nothing personal”* on the shared device rather than contesting the arrangement itself: *“Most of the devices I do share. . . I don’t have personal information on there”* (S37). The few who described sharing as “reasonable” or “comfortable” nonetheless voiced an underlying desire for more privacy and reported relying on protective strategies of their own: *“I’ve had to log out occasionally*

like I've logged out of Instagram" (D33), and *"I should have more privacy... when they always check my phone"* (D33, S37, D24), despite having just described their own sharing as comfortable. 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). Across all three patterns, dependents' stated comfort was frequently contradicted by their own behavior: even those who reported feeling "fine" with sharing routinely cleared browsing history, logged out of accounts, or avoided storing personal content on the shared device altogether, suggesting these protective habits reflected a persistent, if unspoken, discomfort that self-reported comfort levels alone did not capture.

5.2.3 Financial Loss as the Lens for Security

Across almost all families, financial harm was the risk parents named first, most consistently, and with the most concrete detail. Many parents described a shift toward digital, phone-mediated banking after migration, with little precedent in their countries of origin. As one father put it, reflecting on life after arriving in Canada, *"Most of the banks were online. Everything was digital... I got more dependent on my phone to get out of the house"* (M17).

Parents' working model of "security" tended to equate protecting money with protecting the family more broadly, leaving related but non-financial credentials comparatively unguarded. One father described a financial scare as fully resolved by a single reactive step: *"If it is something to do with my bank[ing] information, I just block my card and call the bank... other than that, I never had any other such problem"* (M12). Another mother described avoiding digital payment methods altogether as her primary safeguard: *"I don't use a digital card... I use a physical card"* (M18), treating the elimination of a payment format, rather than the credentials protecting the accounts behind it, as the meaningful boundary.

Because children's routine activity on shared devices could translate directly into financial exposure, several families introduced approval-based purchasing as a structural control rather than relying on supervision alone: *"If they want to purchase something, they have to send a request and I have to approve it"* (F4). Yet this same vigilance rarely extended to the accounts that made purchasing, banking, and password recovery possible in the first place. One father described a banking app that closed automatically on a shared device, then immediately undercut that protection by describing his email as persistently accessible from any device in the house: *"Banking [app] automatically close[s]... regarding my email address, you can open it here, you can open it in the other device, it's already saved"*

(F3). Because email accounts typically mediate password resets and account recovery for banking and shopping alike, this left the single point of failure, open even in households that considered themselves financially cautious. Families reserved their most concrete protective behaviors for money itself, while the credentials and accounts guarding access to that money were frequently treated as a lower-stakes, and in practice unprotected, adjacent concern.

5.2.4 Child Originated Threats

Seemingly low-stake risks initiated by dependents on shared devices can escalate to household-level Security and Privacy threats due to the interconnected nature of banking, school, social media, and email accounts.

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 [5]. Such incidents may be read as inappropriate behavior, affecting reputation within communities in Canada or in their home country [5].

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 [49]. 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.

Not all child-originated risks were malicious or high-stakes: dependents also described curiosity-driven actions with lower consequences, such as prank-calling a pizza restaurant from a parent’s phone (D20) and opening and reading a sibling’s or friend’s chat simply “to

see what they were talking about” (M10). These incidents illustrate that shared-device risk exists on a spectrum from mundane curiosity to genuine harm, and that not every boundary violation reflects an intent to deceive.

Stranger Danger: Beyond everyday friction over shared accounts and visibility, families also described more serious risks tied directly to contact with strangers online. Parents did not treat such contact as a minor inconvenience, but as a direct pathway to physical, financial, or sexual harm, including grooming, blackmail, and exploitation. One parent described a particularly alarming exchange her child had received: *“Somebody kept asking them, ASL, ASL, your age, sex, location... And then I told them, your age, your sex, and your location are private matters. We don’t tell these to strangers”* (M9). These fears were especially pronounced for daughters; one parent linked unsolicited online flattery directly to a manipulation attempt involving her eleven-year-old: *“He said that you look beautiful... so she turned on the camera”* (M12). Notably, several parents described deliberately withholding visible reactions to these disclosures in order to keep their child’s willingness to disclose intact: *“She was scared a little bit... I did not react because I’m scared that then they will stop telling me all these things”* (M12). Stranger-contact risk operated not as an abstract concern but as a concrete, frequently anticipated threat that shaped both the restrictions parents imposed on dependents.

“Friend Equals Safe”: Many children’s safety judgments on shared devices relied less on technical assessment than on a simple heuristic: familiarity was treated as a proxy for safety. As one participant explained when deciding whether to click a link or accept a request, *“’cause I usually trust my friends with that... I was just like, ‘Yeah, sure, why not?’”* (D26). This heuristic frequently blurred the line between legitimate communication and social engineering. One participant described losing access to their own account after being deceived by someone posing as a friend: *“Pretending to be my friend... I thought they were my friend... so I gave them my account and then that’s how I got hacked”* (D21). The same logic extended to sharing credentials directly: *“If it’s my friend I’m gonna click it”* (D25); *“Yeah, I share my lock screen password”* (S41). Because shared-device immigrant households already normalize a degree of access-sharing within the family, this heuristic may generalize unusually easily to peer relationships, leaving children with comparatively few independent cues for evaluating risk before extending that same trust outside the household.

The children’s post-interview survey suggests this heuristic is not only about judging external risk. Asked how comfortable they felt when different people used their personal device (1 = Extremely Uncomfortable, 5 = Extremely Comfortable), participants reported feeling more comfortable with a close friend using their device ($M = 3.41$) than with their parent ($M = 2.86$), sibling ($M = 2.80$), or another family member ($M = 2.23$, the

lowest of any category). Family members, not only external actors, appear to be the more privacy-invasive audience in everyday experience.

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.

5.2.5 Security and Privacy Workarounds for Device-Sharing

We identified five overarching Security and Privacy 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 5.3.



Figure 5.3: Security and privacy challenges and safeguards in shared-device households.

Families relied on risk-avoidance and ad hoc concealment tactics to manage Security and Privacy 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.

Different Priorities for What Is “Private”: Privacy priorities differed by role. Children sought to protect social spaces such as chats, photos, and browsing history, while parents focused on banking, email, and account security. Table 5.2 summarizes the information types each group most frequently named as needing protection.

Table 5.2: Participants Information Protection Concerns during Device Sharing.

Information type	Children (c)	Parents (p)	Total (%)
Communication content (messages, chats, email)	9	8	41
Authentication credentials (passwords, logins)	8	7	36
Personal identifying information (address, phone, photos, name)	8	8	39
Online stranger interaction	10	9	46
Suspicious links and downloads	7	7	34
Financial information and transactions	3	8	26
Browsing history and viewed content	6	5	26
Device use monitoring and activity visibility	5	6	26
Work or professional information	1	5	14
Saved sessions and credential persistence	5	5	24

Dependents: Dependents emphasized personal chats, photos, and privacy-sensitive browsing as key concerns on shared devices [173]. Our findings on password sharing align with prior work [159, 171]. 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). This regulation extended beyond digital spaces to include curation of friends and family social circles in Canada: "*We make sure... are on the same page when it comes to parenting... religion derives a lot of values in my life*" (M10).

Hiding as a Guilt Signal: Within several households, children's attempts to assert even minimal privacy were routinely interpreted by parents as evidence of wrongdoing, rather than as ordinary boundary-setting. As one child explained, "*That just goes to show like, oh I'm hiding something and that will make them even more concerned*" (D33). Even the act of verbally requesting privacy could backfire, deepening rather than resolving parental suspicion: "*If I told them not to open it, that would keep them suspicious... then they'd think, 'why is she saying don't open it?' That creates more suspicion*" (D28). Several children described this dynamic as self-reinforcing, in which privacy itself was treated as inherently suspect: "*[Parents think that privacy is a privilege because] at the end of the day, you shouldn't be doing anything that requires that much privacy*" (D33). Parental monitoring in these households also operated through sudden, unannounced checks that reinforced control through unpredictability rather than through any stated rule: "*My mom snatched my phone, I was like, why are you not respecting my privacy? I just had that out of like anger. And she was like, oh, that's not even real. Like, shut up. Like, what are you talking about?*" (S40).

"You Wouldn't Understand": A related but distinct motivation for concealment was not guilt but a perceived inability of parents to correctly interpret ordinary digital content. Dependents described withholding jokes and messages not because the content was unsafe, but because they anticipated it would be misread as inappropriate. One

daughter described a meme a friend had sent her that her parents saw on a shared email account: *“It’s like a generational gap... it was like a gen alpha type meme... it’s funny to me and my friend, but... in my parents’ eyes very inappropriate”* (D20). Rather than risk a conflict she considered disproportionate to the content itself, she declined to explain the joke, anticipating that her parents would “get mad” regardless of the explanation.

This dynamic recurred across households, particularly around the hyperbole and exaggeration common in adolescent peer communication. One daughter recalled being challenged for joking with friends using an obviously non-literal statement: *“I’m joking around with my friends... [saying] I’m going to jump off the building. Why are you saying this?... it’s just an exaggeration”* (D33). Another described the same concern extending to everyday inside jokes, which she expected would be misread rather than understood: *“we have some inside joke[s] and they wouldn’t understand it without questioning”* (D27) – a pattern the interviewer independently confirmed was common across multiple families in the sample.

For some dependents, concealment in these cases was framed less as self-protection than as protecting the social relationships the content belonged to. One daughter explained that she kept messages with friends private specifically to avoid *“the trust [being] broken over these small things,”* (D29), while still making sure her parents knew who her friends were. Unlike the guilt-signal dynamic described above, in which any act of hiding was read as evidence of wrongdoing, this generational gap in interpretation left dependents concealing content precisely because they judged it harmless.

5.2.6 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.

Table 5.3 summarizes the range of post-hoc strategies families adopted, organized by the mechanism enacted and the incident that typically triggered it. Families rarely pre-configured safety; instead, they reconfigured access only after a breach, scare, or discovery,

shifting from ad hoc concealment to more structural controls (settings, segmentation, monitoring).

Table 5.3: Post-hoc responses to S&P incidents.

Post-hoc response type	Mechanism	Typical trigger	Quotes
Concealment upgrade, feature hardening after incident	Clearing history → switching to incognito; hiding traces after being caught	Parents discover activity / child gets in trouble.	<i>“Eventually one time... they found out... I didn’t know... So... I found out what incognito was on Chrome. And then I just used that.”</i> (S36)
	Turning off chat, tightening settings, parental controls; incognito for sensitive tasks; avoid installing banking apps; log out	Discovery of chat with strangers / unsafe defaults; fear of kids accessing financial/personal apps	<i>“checked... parental controls... chat settings... ticked... options...”</i> (M10) <i>“use incognito... no track...”</i> (F5)
App removal / churn / avoidance	Delete/uninstall and sometimes reinstall (TikTok, unsafe apps); removing WhatsApp Web/Desktop logins, uninstalling mirrored apps	Inappropriate content; risky features; conflict; child could read messages on a shared-machine login	<i>“I just like leave that app then... like... delete the apps... and... find another one maybe for kids.”</i> (D22) <i>“I just deleted that app.”</i> (M12) <i>“I removed that app then... because there wasn’t an option to disable the chat feature.”</i> (M9) <i>“My husband... noticed that the money transferred from his bank account... after that told me do not have bank application on your phone.”</i> (M11) <i>“uninstall the WhatsApp app... so... he doesn’t have access.”</i> (F6)
Security tooling / service adoption	Antivirus installed after hack/scare; financial security service adoption	Malware/hack incident; scary breach	<i>“after this... downloading all the antivirus stuff...”</i> (S36) <i>“I... kept all my financial... products... registered... so I get an alert if... anything suspicious happen.”</i> (F7)

Table 5.3 – continued

Post-hoc response type	Mechanism	Typical trigger	Quotes
Account separation / sacrificial account / device segmentation (“this phone is off-limits”)	Delete account → create a “kid-facing” account; certain devices/accounts never shared	Feed contamination / following strangers; political or unsafe feed; adult content in DMs	“deleted my account and created an account which my daughter will use...” (F2) “I... had my WhatsApp chat logins in my laptop... later I did uninstall the WhatsApp app... so that... he doesn’t have access to it.” (F6) “I did some Google search to figure out what I can do and then I came to know about this feature that I actually can create a separate user account... so I don’t have to compromise my account.” (F5)
Supervision escalation / teaching / learning	Sit together; restrict solo searching	Shock event that could have happened unsupervised; taught about security	“What if I’m not sitting right next to her?... I sit with her.” (M10) “Somebody kept asking them, ASL... and then... I told them, your age... sex... location are private... You never respond...” (M9) “After that we like we learned about it.” (D28)
Formal risk monitoring	Credit/ID monitoring; alerts for new accounts or credit events	Prior fraud or heightened risk awareness post-migration	“I get an alert if... anything suspicious happen.” (F7)
Reporting / escalation	Police/bank disputes, refunds, shutdowns	Financial fraud; major safety incident	“I checked the statement... I filed a dispute... and... I got the reimbursement.” (F7) Fraud narratives (M17)

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. The preference for community-based support over formal or automated resources coexisted with a broader, generalized distrust of technology itself. Several parents described digital devices as inherently addictive, morally risky, and harmful to children’s wellbeing, at times invoking exaggerated health claims to reinforce restriction, such as warnings about permanent eyesight damage from screen use (M9). This framing of technology as an inherent threat, rather than as a tool requiring calibrated use, may help explain why some families gravitated toward blanket restriction and avoidance-based strategies rather than more granular, skill-building approaches to digital safety.

5.2.7 School vs at Home Teaching

Across interviews, we found that children consistently described school-based safety education as easier to understand and more helpful than what they receive at home. While parents often focused on rules and restrictions, children valued the way teachers explained risks with examples and a calmer tone. As one child put it, *“[I prefer] School. I don’t know, I just like school better. They make it more creative and detailed”* (D26). Another added, *“Because in school it helps me understand it better than at home”* (D24). Tone mattered strongly: *“My parents are very strict but my teachers are very kind”* (D30). Even when the content was similar, such as not clicking links or sharing passwords, children felt school guidance was easier to accept and remember: *“They teach us not to click on links and not go on certain games... it’s happened before with some kids”* (D24).

Parents themselves often acknowledged that schools and daycare providers take the lead in digital safety education, sometimes more effectively than families can at home. Several openly admitted that children learn more from teachers than from parental warnings. *“I think the daycare lady and school teach more”* (F1). They described school instruction as structured, scenario-based, and less controlling. As one parent reflected, *“At home it’s more of a controlling approach... school makes them part of the process”* (M10). Repetition at home could lose impact, whereas formal sessions carried authority: *“When you keep telling your child... they don’t end up taking you seriously. But school made it a point that the kids were aware”* (M10). Overall, parents saw schools as better positioned to prepare children for real-world risks rather than relying solely on restriction.

Table 5.4 summarizes what parents reported teaching at home.

Table 5.4: Home-based digital safety teaching by topic.

Topic parents teach	Families
Not talking to strangers online	15/18
Not sharing personal information (address, phone, photos)	13/18
Avoiding suspicious links or downloads	11/18
Password and account protection	10/18
General cautionary rules (“be careful,” “don’t do this”)	8/18
Teaching triggered after a negative incident	8/18

5.2.8 Reverse Mediation:

Section 5.2.7 documents a one-directional flow of safety knowledge, school and parents teaching children, and finds children rate school instruction as clearer and less controlling. Our data contains a second, opposite flow as well: Dependents as Household Digital-Safety Educators.

A teenager, for example, described actively building her mother’s threat literacy around AI-generated content, on top of setting up shared home security infrastructure with her: *“we set up our home security cameras together, so I make sure they know how to use it anyway... facebook has a lot more of like those fake news we talk about... ai videos we talk a lot about, that a lot to be like i just have to make sure with my mom like, you this is ai right? she’s like yeah but like just to make [sure]”* (D33). Asked directly whether she felt she understood online safety better than her parents, she confirmed it without hesitation: *“yeah i feel like i watch a lot more stuff about that too... sometimes i hear about the scams on tiktok so i think about it a little bit more”* (D33). Another dependent, asked the same question, gave a similarly concrete example rather than a general claim: *“like being misled by AI”* (S39), naming it as the risk category he had to explain to his parents.

A third participant extended this from AI content to financial scams, again naming the specific gap rather than a general competence claim: *“there’s a lot of things they don’t really know, there’s like scam... AI scams, like videos of people and stuff like that that they think are actual people. I can imagine that’s not a real person, that’s an AI. So I wouldn’t trust what they’re saying about stuff”* (D21). Another dependent similarly described teaching

her parents, *“I was like, that, don’t like these things, it might get you in trouble”* (D29).

This pattern is well documented in immigrant-family research under “language brokering”, children translating language and institutional systems for parents who are still acquiring them. What we find here is closely analogous but specific to digital-safety literacy: children, who typically acculturate to new platforms and threat types faster than their parents, become the household’s de facto AI- and scam-literacy educators, inverting the top-down mediation model.

5.2.9 Say-Do Gaps in Privacy Practice

Section 5.2.2 notes in passing that dependents’ self-reported comfort with sharing was frequently contradicted by their own behavior. Our data supports treating this as a pattern in its own right rather than a footnote, and it appears on both sides of the parent-child relationship, not only among dependents.

One father, asked what precautions he took before handing a device to his children, described a household with hidden, individually-locked folders and a habit of deleting his own browsing history, then, two questions later, characterized the family as having no privacy practices at all: *“we don’t do much... we live openly, I mean, yeah, we don’t have any issue. We are open family, our culture also like that”* (F3). The self-description of openness sat directly beside a described practice of concealment, with no apparent friction between the two in how he told it. A second parent produced a nearly identical pattern in miniature, first denying that she monitors her adult daughters’ phones at all, then immediately qualifying it into its opposite: *“No, no... before eighteen, yes, sometimes I check what they’re doing with their phone... even at that time, with their permission”* (M11): a flat “no” that resolves, within the same breath, into “yes, regularly, for years.”

Dependents showed protective behavior paired with an explicit denial that there was anything to protect. One teenager described using an app lock on nearly every application on his phone *“’cause I wanna make sure that if say someone steals my phone, I’ll be able to control what apps they can and can’t use”* (S35), a real, actively maintained security measure, while separately describing himself to us as someone with nothing on his device his parents couldn’t see. Another dependent gave the same shape of answer about hidden apps: *“I do have hidden apps, but deleting chats only when my story is full, not because someone has to read it. I don’t have anything in private”* (F6): hidden apps and a “nothing in private” claim delivered in the same sentence, with no sense that the two might be in tension. A third dependent drew a finer distinction: she reported no discomfort with monitoring in the abstract, but real, physical anxiety at the fact of being checked

regardless of whether anything incriminating was found: *“I don’t feel anxiety... it’s like an uncomfortable feeling”* (D29) even when a parent was “just getting help” on the shared device, not searching it.

These suggest that “nothing to hide” functions in these households less as a factual claim about device contents and more as a relational script: a way of affirming trust and family harmony verbally, which coexists comfortably with private, individually maintained protective behavior that never has to be reconciled with it out loud. It suggests that behavioral proxies, app-lock adoption, history-clearing frequency, hidden-folder use, may be a more trustworthy signal of a household’s actual privacy need than stated comfort levels alone.

5.3 (RQ3) What Makes Sharing Safe

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 Security and Privacy tools for device sharing(5.3.2), advice for families(5.3.3 and design needs 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 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 (e.g., 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).

Family and Community as the First Line of Help. When facing an unfamiliar security or privacy problem, participants turned first to people they already trusted rather than to a device’s built-in support resources. Several parents identified a specific relative with technical expertise as the household’s default troubleshooter, concentrating both technical authority and rule-making authority in one person. One mother explained simply, *“it’s my husband. He’s the IT person, and he does a lot”* (M18), while a son from another family similarly deferred to his father’s professional background: *“I say it more my dad because he does work in IT... so I trust his [judgment on] what he knows about it, for [making] rules”* (S35).

Where no household member had relevant expertise, participants extended the same trust outward to relatives and community members who shared their cultural background, rather than to search engines or institutional resources first. One mother described relying on a family member studying in a technical field: *“I end up calling my Khala [aunt]... she’s majoring in computer science[s]... I feel she’s very confident [in her abilities]”* (M10). Another father described this as a broader community norm rather than an individual preference: *“something happened, we share in our community, and you come to know”* (F3). For at least one family, this informal network was supplemented by formal newcomer-oriented programming: a daughter recalled attending *“workshops for newcomers about... internet safety”* run by a nonprofit organization shortly after arriving in Canada (D28).

AI as a Supplementary Safety Check: Across immigrant households, AI tools were used cautiously and selectively, typically as low-stakes, first-pass resources rather than trusted authorities. Some parents avoided them entirely due to concerns about psychological harm and opaque data practices, citing reports of children being negatively affected, including a widely discussed case linked to suicide (*“we know the danger of technology,”* F1). We found that AI was largely confined to non-sensitive tasks such as entertainment or basic problem-solving. Participants described using AI as a quick, first-pass check to gauge whether an app or situation might be safe, while deliberately limiting reliance and verifying information through other sources like Google due to concerns about misinformation and data misuse. As one participant noted, they might ask AI for a *“general... look over all the reviews,”* but still *“look at the reviews yourself”* (S38). Others framed AI as convenient but unreliable, ranking it below search engines and treating it *“with a grain of salt”* (F5,S35).

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 5.2.4, 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. Parents' own reported barriers to managing devices were rarely about raw digital skill: only 29% cited low digital literacy as a barrier, 21% cited a child being too young to use a device competently, and 14% cited low confidence or anxiety around technology, consistent with a sample in which 94% held a bachelor's degree or higher.

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.

Practicing What You Preach: A third strand of parental advice centered not on rules for dependents but on parents' own conduct as the more persuasive lesson. One mother described this directly, framing verbal instruction as secondary to what children actually observed at home: *"Kids just follow but they see. A lot of time it's just that passive learning that's happening throughout the house... it's not always what you're saying, mostly it's what you're doing"* (M10). Another parent described deliberately narrating his own compliance with household rules so his children would recognize the rules as shared rather than one-directional: *"You have to tell the kids, I have completed so many tasks, that's why I am watching TV. Then the kids feel that the parents are also following the same rules"* (M17).

The same parent extended this logic to substituting supervised, screen-adjacent alternatives for unsupervised device time rather than removing screens outright. To keep his children occupied without giving them his phone, he described providing a tablet restricted to schoolwork (*"they will only use the tab to do their children's work... they don't use devices without supervision"*), and, for entertainment, replacing television with an audiobook

app used during shared chores: *“Instead of watching TV, I put an audio book on it... boring work becomes interesting”* (M17). These examples suggest that some parents treated safer sharing as something to be demonstrated and structured into shared routines, not only enforced through rules directed at children.

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. The requests therefore centered on making shared devices function as safely shared spaces rather than personal, single-user devices. We group these requests into five overarching categories, given in Table 5.5.

Table 5.5: Participant Reported Design Needs.

Category	Requested Design Features	N
Proactive Monitoring & Alerts	Real-time warnings for unsafe sites, sensitive data entry, purchases, or unauthorized account access; dependent’s screen-time alerts for parents; approval prompts on account/data access.	8
Granular Privacy & Selective Sharing	Per-app locks, temporarily hiding apps from view through visibility filtering, stealth histories, discreet usage masking, and limited app-only access without exposing the full device.	11
Parental Governance & Remote Management	Granular app/device permissions and parental controls, strong age- and faith-based content filtering, foolproof and centralized parental controls across operating systems, app safety ratings on app stores, remote access to the dependent’s device, and user-based activity logs.	5
Identity-Aware Access	Automatic biometric recognition that loads the correct family member’s device profile, including apps, history, and logins; trust-based access levels; and auto-lock for unrecognized users.	12
Multi-User Profiles	Multi-profile phones with automatic session switching and isolated apps, storage, and data to prevent cross-account mix-ups between users.	18

1) Identity-aware access (requested strongly by both groups) 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). Participants wanted devices to recognize who is using them and

automatically load the correct family member’s profile on login, as a safeguard against unrecognized or unauthorized users.

2) Strict multi-user profile separation (requested strongly by both groups), to prevent issues and conflicts explained in Section 5.2.2. Families called for multi-profile phones with strict separation of apps, storage, and data across users to prevent these issues.

3) Parental controls unified across operating systems (requested by parents), 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). Parents requested centralized parental controls across operating systems and filtering aligned with family values and religious expectations.

4) Real-time safety alerts (requested strongly by parents) due to risks like accessing another users data, or dependent accessing culturally inappropriate content, explained in Section 5.2.4. Participants wanted real-time alerts and warnings for unsafe sites, sensitive data entry, purchases, or unauthorized access.

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). Families emphasized the ability to share specific apps or functions while keeping personal content hidden from other household members. Together, they sought support for making cultural device-sharing practices safer.

Together, these findings show that shared-device security and privacy cannot be understood only in terms of individual users, device settings, or technical protections. Participants’ experiences were shaped by family roles, expectations of trust, parental responsibility, dependence, and culturally grounded ideas about appropriate access and oversight. The next section draws these findings together to examine what they mean for how shared-device privacy is understood and how future systems might better support the needs of collectivist immigrant families.

Chapter 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, contradicting their claim, they also acknowledged its risks and challenges as discussed in Chapter 5, revealing many tensions in practice. Some Parents dismissed privacy by claiming it is “not even real” to justify unannounced monitoring, reinforcing parental authority in ways dependents found discomfiting and disturbing; demonstrating that challenges operated in both directions.

A recurring challenge when conducting this study was disentangling the influence of religiosity, immigration, and home-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 practices, 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 question parents, were forced to comply and expressed discomfort with parental sharing norms [159, 34]. This constrained voice can aggravate privacy harms and disturb family peace, breeding grudges, emotional distance, and leading to hidden activity and risky workarounds putting the 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. 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 5.2.4). 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 [119, 32, 18]. Our findings align with prior work on norms of modesty [49]; we found that anxieties about women’s online visibility, cross-gender interaction, and reputational harm appeared across multiple religious groups. Device sharing reinforced gendered hierarchies, framing privacy as collective accountability to family rather than individual autonomy [115]. Participants also noted that current parental controls often fail to reflect faith-based distinctions and requested more of such features in devices (Section 5.3.4). These findings motivate Security and Privacy and HCI research on shared-device designs that better support collectivist and faith-based practices, while carefully avoiding designs that reinforce surveillance for an already at risk group.

6.2 Teaching Avoidance, Not Understanding

Across families, parents tended to frame children’s digital safety education around protecting innocence rather than building judgment. This often meant limiting exposure rather than openly explaining the reasoning behind a restriction: *“I don’t want to take away her childhood innocence...but the world works that way”* (M10). Where safety guidance was offered explicitly, it was typically delivered as categorical, rule-based warnings: do not talk to strangers, do not share information, and do not click links. These warnings emphasized avoidance more than the development of independent risk judgment.

This teaching was also largely reactive. As discussed in Section 5.2.6, families described intensifying safety conversations only after an incident had already occurred, rather than building proactive understanding beforehand. These conversations also tended to focus narrowly on a small set of recurring threats, rather than equipping children with transferable and evaluative skills. When considered alongside the “friend equals safe” heuristic described in Section 5.2.4, this avoidance-oriented teaching style may help explain why children’s own risk judgments relied so heavily on social familiarity rather than independent technical assessment. When safety is taught primarily as a list of things to avoid, rather than as a skill to develop, children are left with few tools for evaluating the much larger space of risks that the list does not anticipate. These findings echo recent policies, like Australia’s under-16 social media ban policy [22]. However, our findings suggest that avoidance-based approaches alone may be insufficient in shared-device households, where dependents’ access to digital technologies cannot always be eliminated without disrupting established household sharing practices. Rather than relying primarily on families to restrict access, platforms could provide protections that reduce dependents’ exposure to harmful content and interactions during use. This is especially important in our context, where device sharing is embedded in everyday family practices and families cannot simply remove phones or avoid sharing them.

6.3 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 limited options, poor usability of these features, and misalignment with household sharing practices which makes them non-existent despite being present as seen in prior work about password managers [57, 124]. 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 [12]. 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 [9]. 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 [162]. One possible direction towards this could be preset profile and parental-control templates that offer adjustable starting points, reducing setup burden on parents while also preserving flexibility.

Device sharing is not unique to immigrant families and extends to lower-income or resource-constrained households globally, even in the west [85, 41]. Our sample skews relatively educated and tech-savvy population, 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 the challenges faced by less tech-savvy or lower-income immigrant households are possibly even worse. 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 [35]. Our contribution is to examine shared-device use within collectivist immigrant families, where limited support, reputational sensitivity, and filial duties, and migration constraints make sharing more entrenched and consequential.

Table 6.1: Mapping of Device-Sharing Challenges, Participant Articulated Desires to 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

6.4 From Challenges to Goal State

Our findings suggest that tensions in immigrant shared-device households reflect mismatches between institutional technology assumptions and everyday family practices. We found that parents struggled to balance home-culture values with Canadian social norms consistent with prior work [159] and sharing disrupted these contextual boundaries [159, 116]. Beyond physical migration, parents described a form of digital immigration [163]: 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 a particular group.

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 complete autonomy and separation of activity on shared devices. These goals created a persistent tension between oversight and privacy. Even same feature requests by both groups 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 is done in Table 6.1 and 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.

6.5 Future Design Directions

Our five design categories (Section 5.3.4) represent goal-oriented abstractions: each pointing toward a class of solutions rather than defining a single feature. A key insight from our data is that the parent-dependent tension documented throughout our paper does not require resolution at the design level. Rather, a better direction would be one that can hold both goals simultaneously, providing parental assurance without eliminating dependent privacy. We now map some of these design requests to possible directions that future research can investigate, by drawing on our participant accounts.

Identity-aware profile switching: The most consistently requested mechanism across both parents and dependents was automatic separation of data by user, without requiring a full secondary device or a manual lock-screen switch. 65% of children identified “fingerprint or face unlock for certain apps or files” and “phone automatically knows who is using it and only shows their data” as the most meaningful safety improvements. This is not a technically novel concept: Android’s multi-user mode, Xiaomi’s dual-space feature, and Samsung’s app-level biometric locks represent partial implementations already available on commercial devices. The gap is not absence but usability and scope; these features are buried in settings, require manual activation per app, break certain app categories, and offer no sharing support. A more usable implementation could be contextual profile loading: a biometric or PIN at the app level, rather than the device level, that silently loads the appropriate user’s data, without requiring a full device switch. Moreover, full data isolation is neither necessary nor desirable in collectivist households, where some shared visibility is valued. A tiered visibility model, where high-sensitivity categories such as messaging, photos, and banking are user-locked while others such as browser, camera, and dialpad remain shared, could accommodate both dependent privacy and parental oversight within the same session, without forcing a binary choice.

Risk and scam alerts: Current threat alerts are designed for individual users making individual decisions. In shared-device households, the threat surface is compounded: a child clicking a phishing link or downloading malware on a parent’s device exposes the entire household’s accounts and credentials. Our participants cited multiple such cases, such as a child downloading malware on a shared device, generating fears about banking data exposure for the whole family (S36). Yet the device’s existing malware alerts are often addressed to a single user with no indication of household impact. This gap is addressable without new data collection or infrastructure. A safer approach is content alert labels: rather than automatically blocking content, parents receive a notification when a dependent encounters a flagged category. Shared-device risk framing would enable phishing, unsafe download, and suspicious login alerts to surface the multi-user consequence: “This action

could affect all accounts on this device,” or prompt parents about a child’s action. This is both more feasible and more consistent with dialogue-based mediation, which prior work associates with better outcomes for children [44, 156].

Expressive-but-bounded parental controls: Parents in our study did not lack controls as much as they suffered from their fragmentation, inconsistency, and bluntness. Highly educated, digitally capable parents still described fatigue and confusion navigating platform-specific tools (Section 5.3), and nearly all abandoned controls despite continued need. Two directions address this in a broader sense. First, cross-platform aggregation: a unified household dashboard surfacing activity logs, app installs, screen time, and content flags across devices without per-app configuration. The infrastructure for this already exists within ecosystems such as Google Family Link and Apple Screen Time but breaks at platform boundaries: a child on Android and a parent on iOS cannot share a control layer. The design gap is cross-platform enforcement, and ease of use as stated by our participants. Second, adjustable household configuration templates: pre-set governance profiles, such as “supervised child,” “monitored teen,” and “adult,” that bundle common configurations as adjustable starting points, reducing setup burden for parents while preserving flexibility. This is analogous to the safe-search toggle already built into most browsers, extended to a household governance layer.

Overall, these design directions show that shared-device privacy cannot be treated as an individual problem only. In the families we studied, privacy and safety were shaped through family relationships. Future designs should therefore support both needs at the same time. Instead of forcing families to choose between full parental control and full privacy, systems should allow partial separation, flexible visibility, and clearer warnings about shared risks. This would make shared-device use safer without making privacy seem suspicious or making safety feel like constant surveillance.

Chapter 7

Conclusion and Future Work

This thesis set out to understand how migration, culture, and family relationships shape the way collectivist immigrant households share digital devices, what security and privacy risks emerge from sharing, and how well today’s devices support device sharing in families. Across 41 interviews with 18 immigrant families, we found that device sharing in these households is not an incidental byproduct of convenience or cost, but a structured, culturally organized practice through which parents exercise authority, transmit values, and manage safety, and through which children negotiate a bounded form of autonomy. That sharing produces security and privacy risks that are distributed unevenly but felt by the entire household at once: a single compromised account, an over-shared password, or one risky download can cascade across every family member who shares that device.

These findings carry implications beyond the population we studied. Designing for marginalized or extreme users often produces solutions that ultimately benefit much broader populations, a pattern well documented in accessibility design known as the curb cut effect, and one we believe applies here strongly. Other populations may similarly rely on shared devices due to economic, infrastructural, or accessibility constraints, including lower-income households with limited access to personal devices and older adults who depend on family members or caregivers for technology use. These contexts further demonstrate that shared-device use is not unique to immigrant households, but reflects a broader set of social and material circumstances. Immigrant shared-device households experience intensified forms of risks that many other kinds of households also face, from cross-account exposure to conflicts over intentional or accidental privacy invasion, which is precisely why they function as such an informative edge case. Systems designed to support safe sharing in these households would therefore likely also benefit mainstream users who share devices only episodically, such as couples with joint accounts, roommates, or friends borrowing a lap-

top, and who encounter similar, if less acute, risks of cross-account exposure and privacy conflict.

At the same time, we treat the design directions proposed in Chapter 6, such as identity-aware profile switching, tiered visibility, cross-platform aggregation of parental controls, and risk alerts, as design hypotheses rather than finished solutions. Each would require thorough co-design with the communities it is meant to serve, legal review specific to each deployment context, and careful harm evaluation, particularly with respect to dependents, who are already the more underprotected party within these households and could be made more vulnerable rather than less by a poorly implemented design intervention. What we believe our findings contribute is not a single best feature, but a clearer articulation of the underlying needs that any such feature must navigate: mechanisms that reduce shared-device tension while preserving family bonds, and that distribute safety more equitably across every member of the household rather than concentrating both the burden of vigilance and the cost of exposure on one or two people. In this sense, our findings offer a foundation for future design interventions by identifying both the design needs and the household tensions that give rise to them.

Revisiting our three research questions in light of these findings, a consistent pattern emerges: the challenges families described stem less from a lack of awareness of security and privacy risks than from a structural mismatch between collectivist sharing practices and device models that are mostly designed with a single user in mind. Parents and children in our study were not naive about risk; they were working around devices that gave them no good options for expressing the kind of shared-but-differentiated trust their households actually needed. Safer shared use therefore requires more than better education or awareness campaigns. It requires stronger system-level privacy protections and more usable features that move beyond single-user assumptions entirely, toward supporting multi-user, culturally situated device contexts as a first-class design consideration rather than an afterthought.

Our participants were predominantly first-generation South Asian immigrant families recruited through a specific set of channels, so an important next step is extending this work across more diverse socioeconomic, immigrant, and religious settings to test which of our findings reflect broadly shared dynamics of multi-user device sharing and which are specific to the cultural and migration contexts we studied. Doing so would help disentangle culturally specific dynamics, such as the religiously inflected forms of moral screening we documented, from constraints that arise more generally whenever multiple people share one device, regardless of culture. Future work should also prospectively evaluate the design directions proposed here, ideally through co-design studies with affected families, to clarify concrete design requirements and to assess whether these mechanisms reduce household

tensions in practice rather than simply relocating them. Finally, because our findings point to dependents as the consistently more exposed and less protected party in these households, future research should give particular attention to designs that increase dependents' agency and privacy without requiring them to fully exit the household's shared, collective practices, since that full exit is neither realistic nor, for most of collectivist families, desirable.

Ultimately, this thesis argues that shared-device security and privacy should be understood not as an individual concern to be solved one account at a time, but as a household-level issue, shaped jointly by culture, migration, trust, and family relationships. Any device or system that hopes to serve collectivist immigrant families well will need to be designed with that household, and not merely the individual user, in mind. More broadly, designing for these shared-device realities can benefit not only collectivist immigrant families, but also low-income, multigenerational, and other households where device sharing remains an everyday necessity.

References

- [1] Security Behavior Intentions Scale (SeBIS). <https://dl.acm.org/doi/10.1145/2858036.2858265>.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do Not Embarrass: Re-examining User Concerns for Online Tracking and Advertising. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, New York, NY, USA, 2013. Association for Computing Machinery. doi.org/10.1145/2501604.2501612.

- [7] Sirwan Khalid Ahmed, Ribwar Arsalan Mohammed, Abdulqadir J. Nashwan, Radhwan Hussein Ibrahim, Araz Qadir Abdalla, Barzan Mohammed M. Ameen, and Renas Mohammed Khdhir. Using thematic analysis in qualitative research. *Global Media Journal*, page Article 100198, 2025.
- [8] 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.
- [9] 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.
- [10] Syed Ishtiaque Ahmed, Steven J. Jackson, Maruf Zaber, Mehrab Bin Morshed, Md. Habibullah Bin Ismail, and Sharmin Afrose. Ecologies of use and design: individual and social practices of mobile phone use within low-literate rickshawpuller communities in urban Bangladesh. In *Proceedings of the 4th Annual Symposium on Computing for Development*, ACM DEV-4 '13, New York, NY, USA, 2013. Association for Computing Machinery. doi.org/10.1145/2537052.2537066.
- [11] Syed Ishtiaque Ahmed, Maruf Hasan Zaber, Mehrab Bin Morshed, Md. Habibullah Bin Ismail, Dan Cosley, and Steven J. Jackson. Suhrid: A Collaborative Mobile Phone Interface for Low Literate People. In *Proceedings of the 2015 Annual Symposium on Computing for Development*, ACM DEV 2015, London, United Kingdom, December 1–2, 2015, pages 95–103. ACM, 2015. doi.org/10.1145/2830629.2830640.
- [12] 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.
- [13] 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.

- [14] 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.
- [15] 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.
- [16] Amanda Alencar. Refugee integration and social media: a local and experiential perspective. *Information, Communication & Society*, 21(11):1588–1603, 2018. doi.org/10.1080/1369118X.2017.1340500.
- [17] 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.
- [18] Irwin Altman. *Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole, Monterey, CA, 1975.
- [19] Amazon. Alexa Terms of Use, 2021. <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201809740>.
- [20] 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.
- [21] Jacqueline Angella Smith. ”Faith and Fashion: Christian Dress and Identity”. 2021. doi.org/10.32920/ryerson.14644872.
- [22] AP. Australia declares child social media ban victory as 4.7m accounts closed. Al Jazeera, January 2026. <https://www.aljazeera.com/news/2026/1/16/australia-declares-child-social-media-ban-victory-as-4-7m-accounts-closed>.
- [23] Apple Inc. How to Set Up Family Sharing on Your iPhone, iPad, or Mac. <https://support.apple.com/en-us/108380>. Accessed: 14 Feb 2026.
- [24] Remzi H. Arpaci-Dusseau and Arpaci-Dusseau Andrea C. *Operating Systems: Three Easy Pieces*. Arpaci-Dusseau Books, LLC, 1.00 edition, 2015. <http://pages.cs.wisc.edu/~remzi/OSTEP/>.

- [25] Natalia Banulescu-Bogdan. Beyond Work: Reducing Social Isolation for Refugee Women and Other Marginalized Newcomers. Technical report, Transatlantic Council on Migration, Migration Policy Institute, Washington, DC, 2020.
- [26] Natalia Banulescu-Bogdan. Beyond Work: Reducing Social Isolation for Refugee Women and Other Marginalized Newcomers, 2020.
- [27] 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.
- [28] Thierry Bardini. *Bootstrapping: Douglas Engelbart, coevolution, and the origins of personal computing*. Stanford University Press, USA, 2001.
- [29] Thierry Bardini and August T. Horvath. The Social Construction of the Personal Computer User. *Journal of Communication*, 45(3):40–65, 1995.
- [30] 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>.
- [31] 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.
- [32] 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.
- [33] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, MobileHCI '11*, page 465–473, New York, NY, USA, 2011. Association for Computing Machinery. doi.org/10.1145/2037373.2037442.

- [34] Vern L. Bengtson and Petrice S. Oyama. *"Intergenerational Solidarity and Conflict"*, pages 35–52. Palgrave Macmillan US, New York, 2010. doi.org/10.1057/9780230115484₃.
- [35] Angela Glover Blackwell. The Curb-Cut Effect. *Stanford Social Innovation Review*, 15(1):28–33, 2016. doi.org/10.48558/YVMS-CC96.
- [36] Susanne Bødker and Ellen Christiansen. Poetry in Motion – Appropriation of the World of Apps. In *Proceedings of the 30th European Conference on Cognitive Ergonomics (ECCE '12)*, pages 78–84. ACM, 2012.
- [37] Susanne Bødker and Ellen Christiansen. Poetry in motion - Appropriation of the world of Apps. In *Proceedings of the 30th European Conference on Cognitive Ergonomics*, ECCE '12, New York, NY, USA, 2012. Association for Computing Machinery. doi.org/10.1145/2448136.2448152.
- [38] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.
- [39] V. Braun and V. Clarke. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3):328–352, 2021.
- [40] Finn Brunton and Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. The MIT Press, 2015.
- [41] 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/10.1007/978-3-540-74853-3₇.
- [42] 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.
- [43] Britta Busse and Marek Fuchs. Prevalence of Cell Phone Sharing. *Survey Methods: Insights from the Field*, 2013. doi.org/10.13094/SMIF-2013-00004.
- [44] 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.

- [45] 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.
- [46] 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.
- [47] 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.
- [48] Judith Wagner DeCew. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, Ithaca, NY, 1997.
- [49] 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.
- [50] Matías Dodel. Inequalities and Privacy in the Context of Social Media. In *The Routledge Handbook of Privacy and Social Media*, pages 204–214. Routledge, 2023. doi.org/10.4324/9781003244677-23.
- [51] 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.
- [52] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy Expectations and Preferences in an IoT World. In *Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS 17', pages 399–412. USENIX Association, 2017.

- [53] 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.
- [54] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. Transparency for Bystanders in IoT regarding Audiovisual Recordings. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 649–654. IEEE, 2022.
- [55] Victoria M. Esses. Prejudice and Discrimination Toward Immigrants. *Annual Review of Psychology*, 72:503–531, 2021. doi.org/10.1146/annurev-psych-080520-102803.
- [56] Virginia Eubanks. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, Inc., USA, 2018.
- [57] 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.
- [58] Tom Fairless. Immigration Backlashes Spread Around the World, July 2023. <https://www.wsj.com/world/immigration-backlashes-spread-around-the-world-142124bc>.
- [59] David Frohlich and Robert Kraut. The Social Context of Home Computing. In Richard Harper, editor, *Inside the Smart Home*, pages 127–162. Springer, London, 2003.
- [60] 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>.
- [61] 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.

- [62] 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.
- [63] GLOBE Project 2020. GLOBE Project, 2020. https://globeproject.com/about%3Fpage_id=intro.html#globe2020_intro.
- [64] Erving Goffman. *The Presentation of Self in Everyday Life*. Bantam Doubleday Dell Publishing Group, New York, NY, 1959.
- [65] Google Nest Help. Data security and privacy on devices that work with Assistant, 2023. <https://support.google.com/googlenest/answer/7072285?hl=en-GB>.
- [66] Rebecca E. Grinter, W. Keith Edwards, Mark W. Newman, and Nicolas Ducheneaut. The Work to Make a Home Network Work. In *Proceedings of the European Conference on Computer Supported Cooperative Work (ECSCW ’05)*, pages 469–488. Springer, 2005.
- [67] Lea Gröber, Waleed Arshad, Shanza, Angelica Goetzen, Elissa M. Redmiles, Maryam Mustafa, and Katharina Krombholz. ”I chose to fight, be brave, and to deal with it”: Threat Experiences and Security Practices of Pakistani Content Creators. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 19–36, Philadelphia, PA, August 2024. USENIX Association.
- [68] 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.
- [69] Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Too Much Information! User Attitudes Towards Smartphone Sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, NordiCHI ’12, pages 284–287, New York, NY, USA, 2012. Association for Computing Machinery. doi.org/10.1145/2399016.2399061.
- [70] 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.

- [71] 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.
- [72] 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.
- [73] 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.
- [74] 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.
- [75] J. M. Hernandez, E. P. Ben-Joseph, S. Reich, et al. Parental Monitoring of Early Adolescent Social Technology Use in the US: A Mixed-Method Study. *Journal of Child and Family Studies*, 33:759–776, 2024.
- [76] 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.
- [77] 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.

- [78] 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.
- [79] 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.
- [80] 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.
- [81] 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.
- [82] Immigration, Refugees and Citizenship Canada. Fraud targeting newcomers, 2025. <https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/newcomers.html>.
- [83] 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>.
- [84] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E. Grinter. Postcolonial Computing: A Lens on Design and Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, pages 1311–1320. ACM, 2010.
- [85] 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.

- [86] 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.
- [87] 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.
- [88] 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, pages 1647–1650, New York, NY, USA, 2009. Association for Computing Machinery. doi.org/10.1145/1518701.1518953.
- [89] 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.
- [90] 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.
- [91] Margaret Kovach. *Indigenous methodologies: Characteristics, conversations, and contexts*. University of Toronto Press, 2021.
- [92] 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.
- [93] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 3217–3226, New York, NY, USA, 2011. Association for Computing Machinery.

- [94] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 3217–3226, New York, NY, USA, 2011. Association for Computing Machinery. doi.org/10.1145/1978942.1979420.
- [95] Tama Leaver. Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media + Society*, 3(2), 2017.
- [96] Peggy Levitt and Nina Glick Schiller. Conceptualizing Simultaneity: A Transnational Social Field Perspective on Society. *International Migration Review*, 38(3):1002–1039, 2004. doi.org/10.1111/j.1747-7379.2004.tb00227.x.
- [97] Carolyn A. Lin. Exploring personal computer adoption dynamics. *Journal of Broadcasting & Electronic Media*, 42(1):95–112, 1998.
- [98] 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.
- [99] 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.
- [100] Sonia Livingstone, Giovanna Mascheroni, Michael Dreier, Stephane Chaudron, and Kaat Lagae. How parents of young children manage digital devices at home: The role of income, education and parental style. Technical report, EU Kids Online, LSE, 2015.
- [101] Mary Madden. Privacy, Security, and Digital Inequality. Technical report, Data & Society Research Institute, 2017. datasociety.net/library/privacy-security-and-digital-inequality/.
- [102] Mirca Madianou and Daniel Miller. *Migration and New Media: Transnational Families and Polymedia*. Routledge, 1 edition, 2012. doi.org/10.4324/9780203154236.
- [103] Eva-Maria Maier, Leonie Maria Tanczer, and Lukas Daniel Klausner. Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental

Control Apps. *Proceedings on Privacy Enhancing Technologies*, 2025(2):107–124, 2025.

- [104] Shrirang Mare, Aditya Vashistha, and Richard Anderson. Security and privacy design considerations for low-literate users in developing regions. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, 2017. Works-in-Progress poster submission.
- [105] 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.
- [106] Brandy R. Maynard, Michael G. Vaughn, Christopher P. Salas-Wright, and Sharon Vaughn. Bullying Victimization Among School-Aged Immigrant Youth in the United States. *Journal of Adolescent Health*, 58(3):337–344, March 2016. [https://www.jahonline.org/article/S1054-139X\(15\)00704-1/fulltext](https://www.jahonline.org/article/S1054-139X(15)00704-1/fulltext).
- [107] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Interrater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019. doi.org/10.1145/3359174.
- [108] 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.
- [109] 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.
- [110] 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.

- [111] 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.
- [112] 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.
- [113] 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.
- [114] 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.
- [115] 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.
- [116] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA, 2009.
- [117] 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.
- [118] Cliodhna O’Connor and Helene Joffe. Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, 19:1609406919899220, 2020.

- [119] 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.
- [120] 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.
- [121] 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.
- [122] Rizu Paudel, Prakriti Dumar, 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.
- [123] Rizu Paudel, Prakriti Dumar, 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.
- [124] 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.
- [125] S. Punch. Research with children: The same or different from research with adults? *Childhood*, 9(3):321–341, 2002.
- [126] 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.

- [127] Elissa M. Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 920–934, 2019. doi.org/10.1109/SP.2019.00059.
- [128] 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.
- [129] 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.
- [130] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS '18, page 127–142, USA, 2018. USENIX Association.
- [131] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. Inter-mediated 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.
- [132] Patrawat Samermit, Anna Turner, Patrick Gage Kelley, Tara Matthews, Vanessa Wu, Sunny Consolvo, and Kurt Thomas. "Millions of people are watching you": understanding the digital-safety needs and practices of creators. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.
- [133] 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.
- [134] 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.

- [135] 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.
- [136] 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.
- [137] Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri. The Poverty of Privacy: Understanding Privacy Trade-offs From Identity Infrastructure Users in India. *International Journal of Communication*, 12:1228–1247, 2018. ijoc.org/index.php/ijoc/article/view/7046.
- [138] Elisabeth Staksrud and Sonia Livingstone. Children and Online Risk: Powerless Victims or Resourceful Participants? *Information, Communication & Society*, 12(3):364–387, 2011.
- [139] 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>.
- [140] Statistics Canada. Age Categories, Life Cycle Groupings. <https://www.statcan.gc.ca/en/concepts/definitions/age2>, 2024. Accessed: 14 Feb 2026.
- [141] Molly Wright Steenson and Jonathan Donner. Beyond the Personal and Private: Modes of Mobile Phone Sharing in Urban India. In *The Reconstruction of Space and Time: Mobile Communication Practices*, pages 231–250. Transaction Publishers, 2008.
- [142] 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.
- [143] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smart-

phone Usage during the Flight. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021. doi.org/10.1145/3479526.

- [144] A. Strauss and J. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage, Thousand Oaks, CA, 1990.
- [145] Sharifa Sultana, Sadia Tasnuva Pritha, Rahnuma Tasnim, Anik Das, Rokeya Akter, Shaid Hasan, S.M. Raihanul Alam, Muhammad Ashad Kabir, and Syed Ishtiaque Ahmed. ‘ShishuShurokkha’: A Transformative Justice Approach for Combating Child Sexual Abuse in Bangladesh. 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/10.1145/3491102.3517543.
- [146] Sarah Tabassum and Cori Faklaris. Digital Privacy for Migrants: Exploring Current Research Trends and Future Prospects, 2024. <https://arxiv.org/abs/2406.02520>.
- [147] 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, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3715335.3735453.
- [148] 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.
- [149] Reem Talhouk, Syed Ishtiaque Ahmed, Volker Wulf, Clara Crivellaro, Vasilis Vlachokyriakos, and Patrick Olivier. Refugees and HCI SIG: The role of HCI in responding to the refugee crisis. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1073–1076, New York, NY, USA, 2016. Association for Computing Machinery. doi.org/10.1145/2851581.2886427.
- [150] 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.

- [151] 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/>.
- [152] The World Bank. How does the World Bank classify countries? <https://datahelpdesk.worldbank.org/knowledgebase/articles/378834-how-does-the-world-bank-classify-countries>. World Bank Data Help Desk.
- [153] 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.
- [154] Eran Toch, Yang Wang, and Lorrie Faith Cranor. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22(1-2):203–220, 2012. doi.org/10.1007/s11257-011-9110-z.
- [155] Eran Toch, Yang Wang, and Lorrie Faith Cranor. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22(1-2):203–220, 2012.
- [156] 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.
- [157] Harry Charalambos Triandis. *Individualism and Collectivism*. Routledge, New York, 1 edition, 1995.
- [158] Warda Usman, Jackie Hu, McKynlee Wilson, and Daniel Zappala. Distrust of big tech and a desire for privacy: understanding the motivations of people who have voluntarily adopted secure email. In *Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security*, SOUPS '23, USA, 2023. USENIX Association.
- [159] 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.

- [160] Carl A. Waldspurger. Memory resource management in VMware ESX server. In *USENIX Symposium on Operating System Design and Implementation (OSDI)*, pages 181–194, 2002. <https://www.usenix.org/legacy/event/osdi02/tech/waldspurger/waldspurger.pdf>.
- [161] Ashley Marie Walker, Yaxing Yao, Christine Geeng, Roberto Hoyle, and Pamela Wisniewski. Moving Beyond ‘One Size Fits All’: Research Considerations for Working with Vulnerable Populations. *ACM Interactions*, 26(6):34–39, 2019. interactions.acm.org/archive/view/november-december-2019/moving-beyond-one-size-fits-all.
- [162] 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.
- [163] 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.
- [164] Yang Wang. Inclusive Security and Privacy. *IEEE Security & Privacy*, 16(4):82–87, 2018. doi.org/10.1109/MSP.2018.3111237.
- [165] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*, SP ’22, pages 2344–2360, New York, NY, USA, 2022. IEEE. doi.org/10.1109/SP46214.2022.9833643.
- [166] 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.
- [167] 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.
- [168] 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.

- [169] 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.
- [170] Fouzia Younas, Mustafa Naseem, and Maryam Mustafa. Patriarchy and Social Media: Women Only Facebook Groups as Safe Spaces for Support Seeking in Pakistan. ICTD '20, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3392561.3394639.
- [171] 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.
- [172] 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.
- [173] 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.

APPENDICES

Appendix A

Interview Protocols

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?

Appendix B

Household Demographics Form

Before each interview session, the participating parent or guardian completed a household demographics form on behalf of the household. Participation in this form was voluntary, and participants were informed that they could skip any question they were uncomfortable answering. The form was used to collect contextual information about the household and to support sample description and interpretation of the interview data.

Recruitment and Participant Background

1. Participant ID.
2. How did you first hear about this study?
 - University email or department announcement
 - Social media
 - Word of mouth
 - Posters or flyers
 - Other
3. What is your gender?
 - Man
 - Woman
 - Non-binary
 - Prefer not to say
 - Prefer to self-describe
4. How long have you lived in Canada?

- Years
 - Months
5. What is your age?
 6. What is your immigration stream?
 - Family sponsorship
 - International student pathway
 - Refugee
 - Economic/skilled worker
 - Work permit
 - Express Entry/permanent resident
 - Other
 7. How would you describe yourself, in terms of ethnicity? Participants could select all that apply or self-describe.

Education, Employment, Religion, and Language

8. What is the highest degree or level of school you have completed?
9. What is your marital status?
10. What is your current employment status?
11. What is your field of work?
12. What is your religious background? This question was optional.
 - Christianity
 - Islam
 - Hinduism
 - Buddhism
 - Sikhism
 - Judaism
 - Bahá'í Faith
 - Prefer not to say
 - Other
13. What is your country of origin?
14. What languages are spoken at home? Participants could select all that apply or specify another language.

Household Composition and Living Arrangement

15. What is your household's approximate total income before taxes for the past year?
 - Less than \$25,000
 - \$25,000–\$49,999
 - \$50,000–\$74,999
 - \$75,000–\$99,999
 - \$100,000 or more
16. What is the total number of people living in your home?
17. Who currently lives in your home?
 - Spouse
 - Children
 - Parents
 - Other household members
18. How many bedrooms does your household have?
19. Which of the following best describes your current living arrangement?
 - Apartment or condo
 - Townhouse or row house
 - Semi-detached house
 - Detached or stand-alone house
 - Other
20. Do you currently have a personal room or private space at home?
21. Do your children currently have their own room or private space at home?

Device Ownership and Device Sharing

22. What is the total number of people living in your home who share devices?
23. Which of the following smart digital devices are in your home, and how many?
 - Smartphones
 - Tablets or iPads
 - Laptops or desktops
 - Gaming consoles

- eReaders
 - Smart watches
 - Other
24. With whom do you share devices? Participants could select all that apply.
- Children
 - Spouse
 - Siblings
 - Parents
 - Grandparents
 - Other
25. Who is the primary decision-maker for digital rules in your home?
- Father
 - Mother
 - Both parents
 - Elder children aged 18 or older
 - Each individual decides for themselves
 - Parents decide only for children under 18
 - Parents decide for all children, including adult children
 - Other
26. How many of the following digital devices are shared in your home?
- Smartphones
 - Tablets or iPads
 - Laptops or desktops
 - Gaming consoles
 - eReaders
 - Smart watches
 - Other
27. Please rank the device categories from most shared to least shared.
28. How is device sharing managed in your family?
- Devices are shared freely without permission.
 - Everyone sets permissions for their own devices.

- Children need permission to use parents' devices, but parents do not need permission to use children's devices.
- Children and parents both need permission to use each other's devices.
- We have disagreements about device sharing.
- Other

Device-Use Barriers and Privacy Space

29. Do any family members experience difficulty using devices for any of the following reasons?

- Language barriers
- Low digital literacy
- Disability or accessibility needs
- Age-related barriers
- Lack of confidence or anxiety
- Other

30. If parents share a room with children, what is the maximum age of the children with whom they share personal space?

31. If only grown-up children have private space, what is the minimum age at which children have private space at home?