TOWARD STRONGER DIGITAL PRIVACY AND SECURITY: CULTURALLY INFORMED SOLUTIONS FOR SHARED DEVICE USE BY IMMIGRANT FAMILIES IN CANADA

Author: Shanza Shanza (sshanza@uwaterloo.ca)
MMath CS - University of Waterloo

Supervisors: Urs Hengartner (urs.hengartner@uwaterloo.ca)
& Leah Zhang-Kennedy (lzhangkennedy@uwaterloo.ca)

This study investigates the culturally rooted practice of shared device use in immigrant families, revealing critical privacy risks that demand inclusive, culturally responsive design interventions.

MOTIVATION

- **1 in 4 Canadians is an immigrant**, with over 62% from collectivist cultures such as South Asia. In these communities, *privacy is often seen as a luxury*, shaped by norms of trust and family cohesion.
- Device sharing is common due to **economic and cultural norms.**
- This practice heightens privacy risks, especially for women and children with limited control over their data, and **amplifies broader digital threats like discrimination, surveillance, and harassment,** often leading to self-censorship in blurred-boundary, shared-device settings.

"Cultural dimensions are not peripheral to privacy design, they are central. " — Alva et al.

- Children serve as digital intermediaries, helping parents navigate unfamiliar systems but parents and children have distinct threat models:
  - → ***Parents worry about reputation, religion, and visibility***
  - → ***Children focus on scams, misinformation, and data leaks.***

BACKGROUND

"Privacy controls that reflect Western individualistic values are mismatched in environments where devices are used communally."- Sambasivan et al.

- Racialized youth under heavy supervision by parents often **turn to risky workarounds**.
- **Cultural expectations** around **modesty** further limit **women's** digital autonomy, increasing their vulnerability.
- Despite representing a growing population, immigrant families are still treated as **"edge cases"** in most privacy research.

"Security guidance tools assume a baseline of digital fluency and autonomy, assumptions that do not hold in low-income, shared-access environments." - Kostan et al.

- Most **privacy frameworks reflect Western**, individualistic assumptions, personal devices, English fluency, tech-savviness , and even collectivist-focused research often misses shared-device challenges.
- Privacy tools must cater to these issues, supporting inclusive, culturally responsive digital environments where they are **protected, empowered, and visible.**

RESEARCH QUESTIONS

Q1: *What are the **security and privacy perceptions, practices, and needs of immigrant families** in Canada, especially women and children, and how do they navigate digital privacy in shared-device environments?*

Q2: *How do **generational differences and family dynamics** shape the prioritization of privacy and security concerns in immigrant households, and what roles do parents and children play in each other's technology use and safety decisions?*

Q3: *What **socio-technical challenges** do immigrant families from collectivist cultures face in shared-device settings, and how can **privacy and security tools** be adapted to better support their needs?*

OBJECTIVES

Understand how immigrant families manage privacy and security in shared-device settings, shaped by cultural, social, and economic factors.

Identify risks, tensions, and workarounds, especially among women, children, and tech-dependent parents, and map mismatches with current tools.

Develop culturally grounded design principles for future privacy tools, and evaluate a prototype for usability, trust, and cultural fit.

EXPECTED CONTRIBUTIONS

C1: Fills a key research gap by examining privacy in shared-device immigrant households and advancing relational, interdependent models beyond Western individualist frameworks.

C2: Identifies design gaps in current tools and proposes inclusive, culturally aware features, like role-based access and multilingual support, for shared-use environments.

C3: Promotes digital resilience and privacy literacy in immigrant families through open-access dissemination and community partnerships.

METHODOLOGY

Phase 1: Contextual Inquiry

- Semi-structured interviews (1:1 and paired formats)
- Structured questionnaires
- Explore AI usage for privacy/security.

Tools:

- Child-friendly methods: Emoji Likert scales, photo prompts.
- NVivo for thematic coding (e.g., values, behaviors, trust models)

Sample:

- 20–25 families (Collectivist cultures e.g south Asian)
- First and second generation mix
- At least one shared device in regular use

Phase 2: Participatory Co-Designing Solutions & Risk Mapping

- Generate design ideas from Phase 1 themes
- Paper prototyping sessions sketching ideas (e.g., safe zones, family profiles, temporary modes)
- Risk-mapping exercises to visualize data exposure

Participants:

- Subset of Phase 1 families
- Diverse in age, language, and household structure.

Phase 3: Field Testing & Evaluation: Usability, relevance, & trust

- Hands-on walkthroughs (prototype or wireframes)
- Post-study interviews (relevance, comfort, trust)

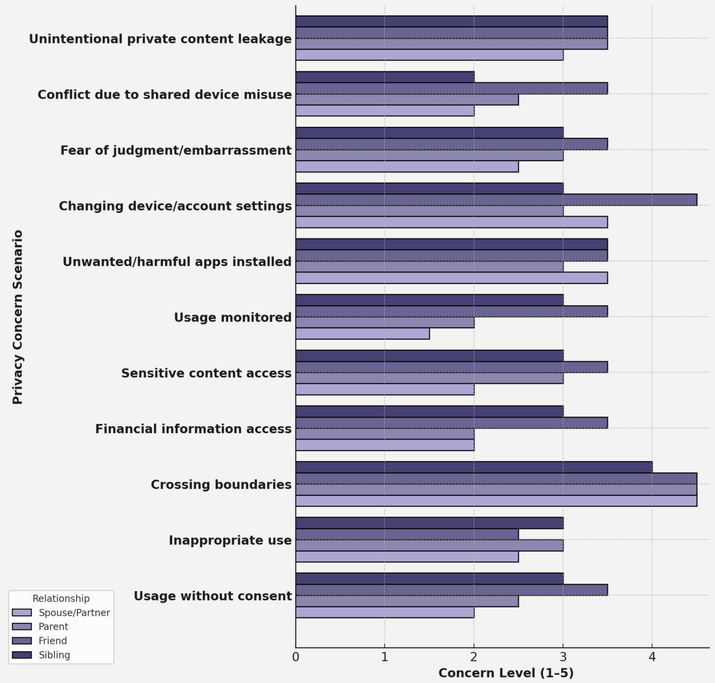
Evaluation Metrics:

- System Usability Scale (SUS)
- Perceived trust (Likert + qualitative)
- Privacy incident reduction
- Cultural alignment score by participants (likert scales).

ANTICIPATED FINDINGS:

- Role-based and session-specific access
- Multi-layered privacy modes by relationship
- Real-time risk and behavior alerts
- Inclusive, low-literacy-friendly interfaces
- Just-in-time, age-appropriate privacy tips
- Intergenerational privacy learning
- Platform flexibility for shared/cross-regional use
- Privacy tools that support trust and autonomy.

Pilot Study Results: Design Gaps in Shared Device Privacy



Pilot survey results: Average privacy concern levels by relationship types

- *Privacy concerns were deeply relational, shaped by trust, family roles, and cultural norms, with financial data seen as most sensitive.*
- *Device sharing was normalized, but created challenges, from usability barriers and indirect risks to cross-regional platform limitations.*
- *Existing privacy tools poorly matched lived experiences, highlighting the need for culturally grounded, multi-user-friendly design.*

Instead of building everything at once, we adopt a scalable, user-driven integration strategy, letting families shape which tools matter most.

LIMITATIONS & PRACTICAL CHALLENGES

- Interpersonal dynamics: Parent- child tensions affect acceptance and use.
- Observer effect: Awareness of being studied may alter digital behavior.
- Recruitment challenges: Hard to reach newcomer or low-income families due to tech and language barriers.