Sharing Digital Devices is Normal and Cultural:

Privacy and Security Challenges in Collectivist Immigrant Households

S. Shanza, Ameemah Humayun, Urs Hengartner & Leah Zhang-Kennedy

UNIVERSITY OF WATERLOO

Full Paper

USENIX SOUPS 2026

Why Collectivist Immigrants?

1 in 4

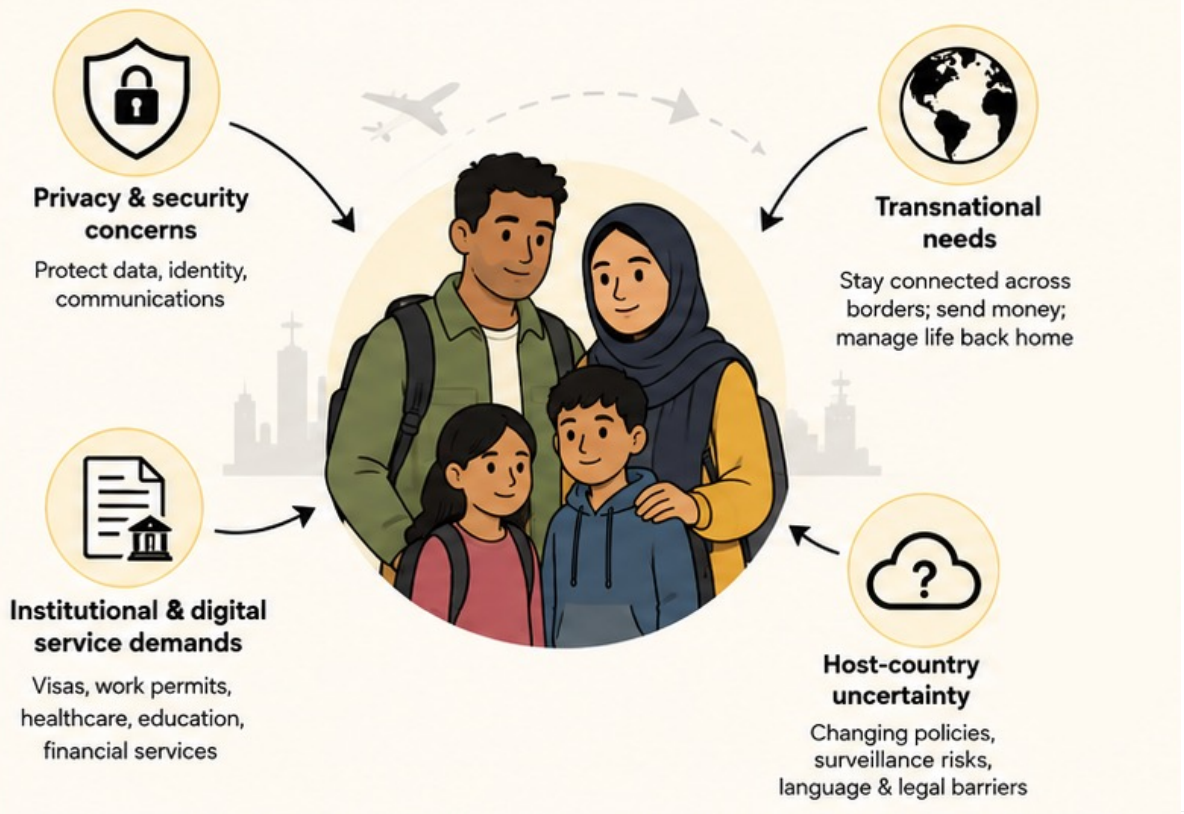
Canadians is an immigrant — many from "collectivist" cultures where digital devices are treated as communal, not personal.

- Life in WEIRD* vs Collectivist contexts[1] [2]
- Strong dependence on technologies post migration[3]
- Discrimination & weak support networks[5]
- High prevalence of sharing = elevated harms[7]
- Privacy is secondary to collective family needs[4]

*WEIRD (Western, Educated, Industrialized, Rich, and Democratic)

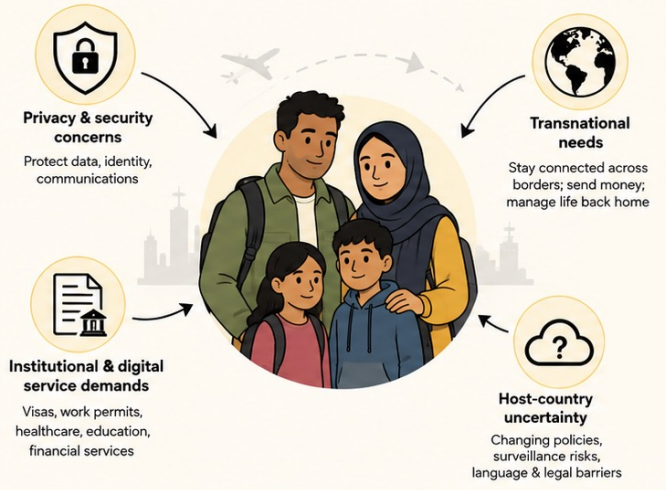
UNIVERSITY OF WATERLOO

Prior Work - Migrants



UNIVERSITY OF WATERLOO

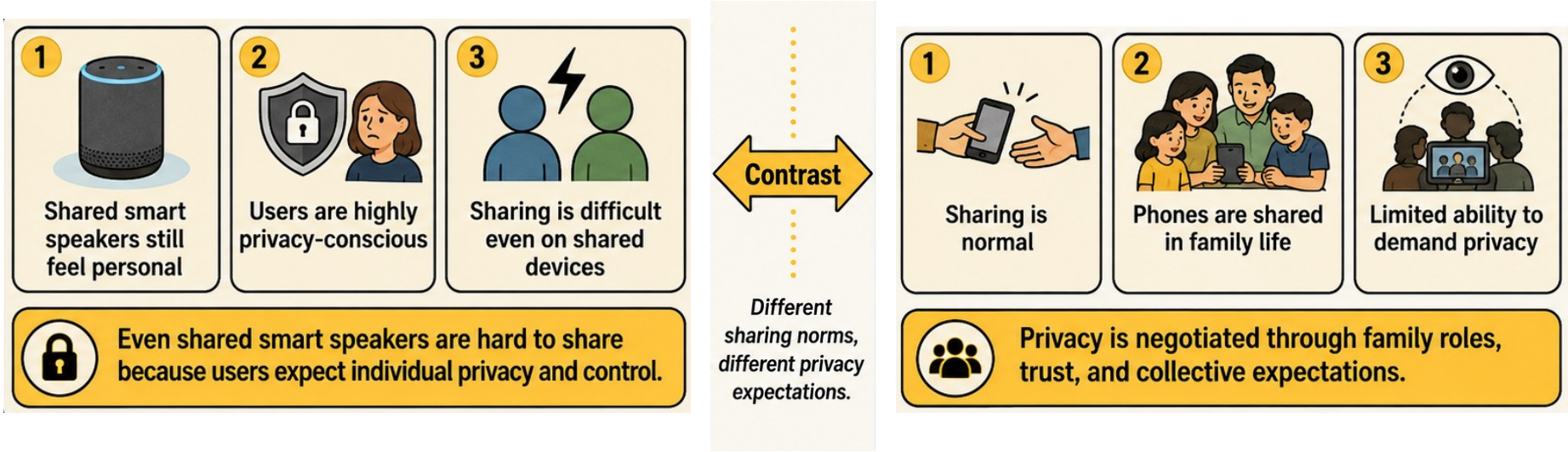
Prior Work - Migrants





UNIVERSITY OF WATERLOO

Prior Work – Device Sharing



UNIVERSITY OF WATERLOO

Literature Gap



Migrant Security & Privacy



Device-Sharing in Collectivist Cultures

UNIVERSITY OF WATERLOO

Literature Gap



Migrant Security & Privacy

This Paper

Collectivist immigrant Families that share Digital Devices.



Device-Sharing in Collectivist Cultures

Research Questions

RQ1

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

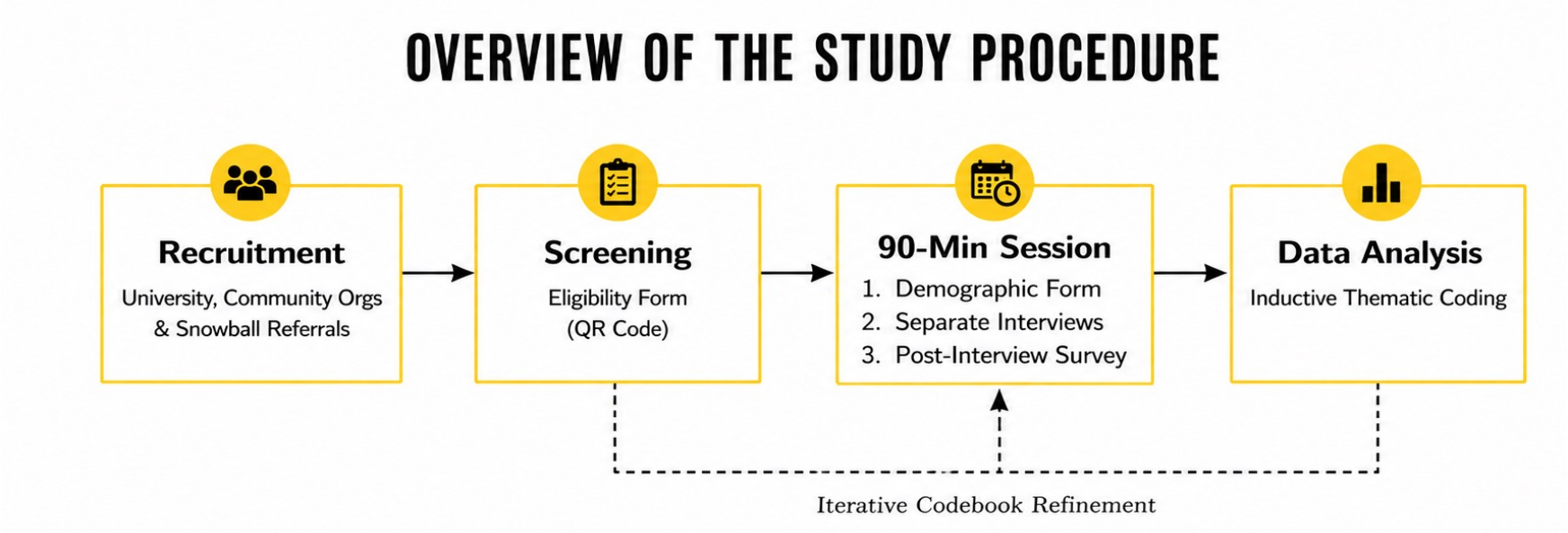
RQ2

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?

Methodology



UNIVERSITY OF WATERLOO

METHODOLOGY

Participant Demographics

41 Participants

19 parents · 22 children & young adults

13/18 nuclear, first-gen South Asian Families

Religion

Muslim (11)

Hindu

Christian (4)

Sikh

Atheist

Country of origin

Pakistan (5)

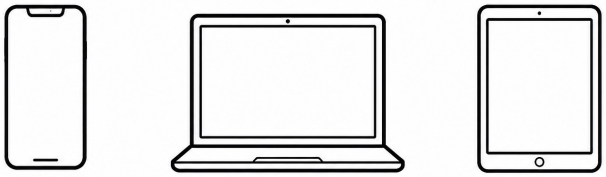
India (4)

Iran(2)

Bangladesh (2)

Ukraine, Zimbabwe, Eritrea, Afghanistan, Palestine

Shared devices



18 Phones

16 Laptops

7 Tablets

UNIVERSITY OF WATERLOO

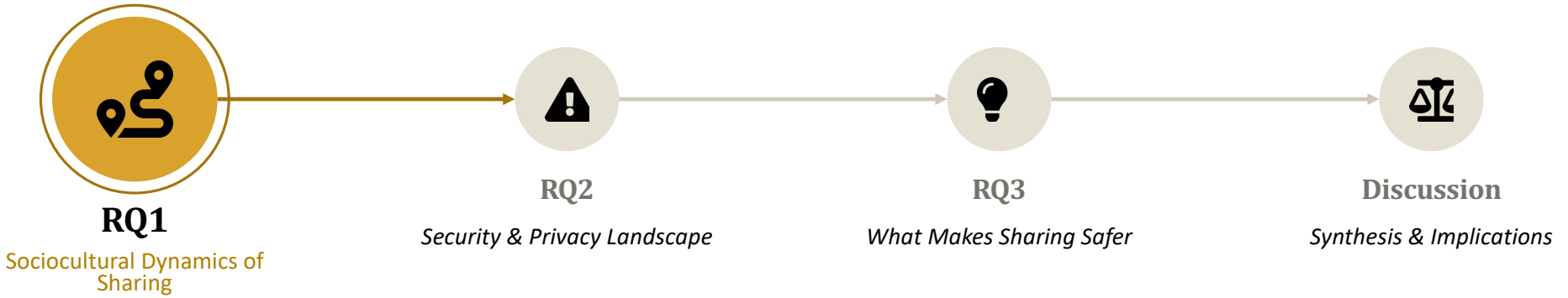
Findings

Why families share digital devices?

Collectivism & cultural norms	Post Migration Safety	Parental monitoring
Coordination	Convenience	Bonding

UNIVERSITY OF WATERLOO

RQ1 — Sociocultural Dynamics and Device Sharing



RQ1

Sharing to avoid Migration caused loss of Supervision

- Migration caused early device access, Reduced oversight & unstructured time post-migration.

> ***"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)***

Devices as Tools for Cultural Transmission

- Parents embedded religious practice into device use

> ***"We have Quran apps... we'd have to read Quran to even use our phones —it's kinda like a reward." (S37)***

- Devices kept in a "morally clean" state (F2)

RQ1

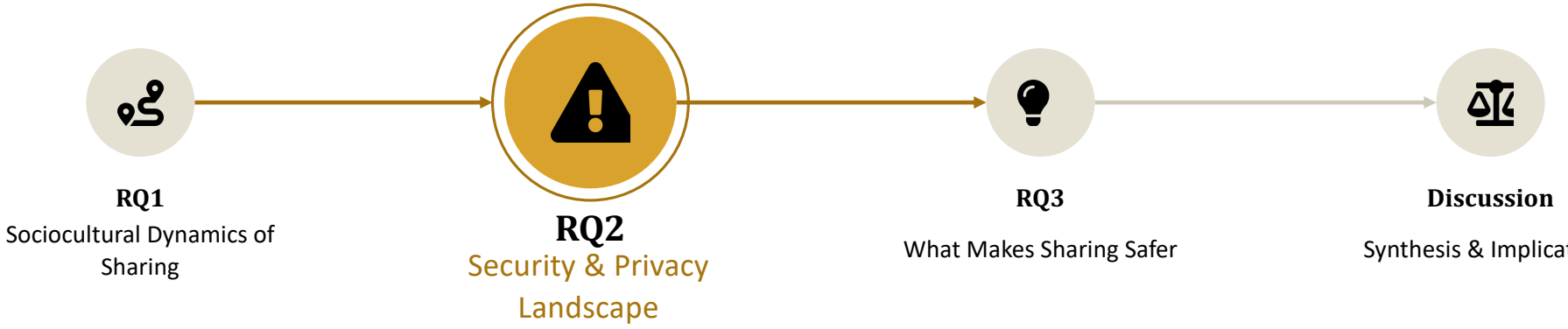
Surveillance, Conflict, and Emotional Strain

"*My parents used to take my phone, and if they didn't approve of something, we would fight about it. This happened a lot*." — D25

- Constant anxiety or stress due to device sharing — D27
- Filters meant for children sometimes blocked mothers' own work access too.

This constrained voice aggravated privacy harms and disturb family peace.

RQ2 — Security & Privacy Landscape



RQ2

Privacy & Security Challenges



Account & Credential Exposure



Intra-Household Privacy Erosion



Social Visibility & Harm



Governance Breakdowns



External Exploitation & Security Threats

UNIVERSITY OF WATERLOO

RQ2

New country, new threats

- Heightened S&P concerns post migration

- Incidents (malware, hacking, harassment) put the whole household at risk

"Somebody called him and asked [my son] to give his passcode… for three or four days it stayed hacked." (M16)

> ***"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, on a deportation-threat scam**

UNIVERSITY OF WATERLOO

RQ2

One device, too many users

- “My dad gets notifications of my Gmail… then he calls my mom and tells her what I’m talking about.” (D26)
- “On phones, we don’t really have separate profiles.” (F2) ·
- Digital traces (chats, history, purchases) sparked misjudgment & conflict among family members.

Algorithmic mixing

One person's activity reshaped content /ads for others on the same device. (M8)

Passive exposure

Shared accounts caused confusion, mixed-up chats, unclear whose data was whose: "*I don't know whose phone I downloaded something on... I'll have to check everyone's phone.*" (D33)

RQ2

Child Originated Harms

- Grooming risk: *"He said that you look beautiful... so she turned on the camera"* (M12)
- Kids judged safety by familiarity: *"I usually trust my friends... why not?"* (D26)
- Child's unsafe action triggered malware in a shared computer (S36)

Faith-Based & Gendered Reputational Harm

- A child texting a mother's boss "I love you" from a shared device (D20)
- "I don't reveal my face, yet my kid put my picture on display on WhatsApp." (M16)
- Daughters face stricter limits on mobility & online activity

Findings

Coping Mechanisms

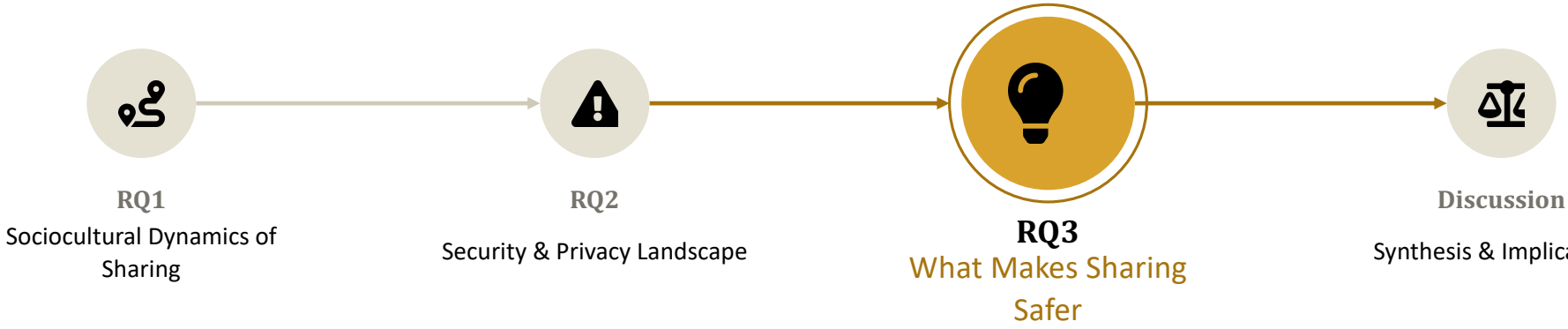
Technical Safeguards (Hard Controls)

- Install–delete cycles
- Disguised/decoy apps
- Removing saved cards or app deletion
- Session cleanup before handover

Behavioral Safeguards (Soft Controls)

- Strict household rules
- Self-censorship per religious/cultural standards
- Active mediation (surveillance, monitoring, talking)

RQ3 — What Makes Sharing Safer



RQ3

Limitations

- "*Nothing makes device sharing feel safer.*" — D26
- Parental controls are burdensome, hard to configure, and easy for kids to bypass.
- Content filtering still surfaced sexual/violent themes even in child-friendly apps:

  "Sonic... someone is beating him... you cannot stop them with a filter.." — F2

- Multi-user features already exist (Android multi-user mode, Xiaomi dual-space) but are buried in settings, requiring manual per-app activation.

PROBLEM: Poor usability and mismatch with real world family needs.

RQ3

What Families Need

Identity-aware access. **(n=18)**
Biometric based switching keeps personal apps and data private.

Proactive alerts. **(n=8)**
Flags phishing, malware & risky content.

Granular Privacy and Parental Governance. **(n=11)**
Manage parental controls and activity logs across operating systems.

UNIVERSITY OF WATERLOO

Discussion

"Device sharing is like… everyone in the family drives the same car… It's a part of life." M17



UNIVERSITY OF WATERLOO

DISCUSSION

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
External exploitation and financial risk	Proactive risk alerts on sensitive activity	High-impact risks are detected without constant monitoring
Unsafe apps / data compromise	App safety ratings in app store	Avoidance of unsafe or deceptive downloads

Conclusion

The curb-cut effect

- Collectivist Immigrant families act as canaries exposing structural flaws in single-user security models.
- Designing for shared-device use by default is essential for more inclusive design that benefits everyone.

- Device sharing is a way of governance, care, and cultural practice.
- A single security or privacy failure can cascade across everyone sharing the device.
- Today's single-user technologies are limited in usability.
- Problems should be translated into underlying needs for shared-device design.

References

1. Usman, Sadik, Taha, Elgedawy, Ruoti & Zappala. *Security and Privacy Experiences of First- and Second-Generation Pakistani Immigrants to the US*. IEEE S&P 2025.
2. Hofstede, G. *Dimensionalizing Cultures: The Hofstede Model in Context*. 2011.
3. Coles-Kemp, Jensen & Talhouk. *In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities*. CHI 2018.
4. Sambasivan et al. *"Privacy is not for me, it's for those rich women."* SOUPS 2018.
5. Esses, V.M. *Prejudice and Discrimination Toward Immigrants*. Annual Review of Psychology, 2021.
6. Statistics Canada. *Immigrant Population in Canada, 2021 Census*. 2022.
7. Ahmed, Haque, Haider, Chen & Dell. *"Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh*. CHI 2019.
8. Mustafa, Asad, Hassan, Haider, Durrani & Krombholz. *Pakistani Teens and Privacy - How Gender Disparities, Religion and Family Values Impact the Privacy Design Space*. CCS 2023.
9. Blackwell, A.G. *The Curb-Cut Effect*. Stanford Social Innovation Review, 2016.
10. Weiser, M. *The computer for the 21st century*. SIGMOBILE Mob. Comput. Commun. Rev., 1999.
11. Parkin, Patel, Lopez-Neira & Tanczer. *Usability analysis of shared device ecosystem security*. NSPW 2020.
12. Steinbrink, Reichert, Mende & Reuter. *Digital Privacy Perceptions of Asylum Seekers in Germany*. Proc. ACM Hum.-Comput. Interact., 2021.
13. Slupska, Cho, Begonia, Abu-Salma, Prakash & Balakrishnan. *"They Look at Vulnerability and Use That to Abuse You."* USENIX Security 2022.
14. Matthews, Liao, Turner, Berkovich, Reeder & Consolvo. *"She'll just grab any device that's closer."* CHI 2016.
15. Meng, N., Keküllüoğlu, D., & Vaniea, K. (2021). Owning and sharing: Privacy perceptions of smart speaker users. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), Article 45, 1–29. https://doi.org/10.1145/3449119

Thankyou.

Full Paper



S. Shanza
sshanza@uwaterloo.ca



Ameemah Humayun
26100175@lums.edu.pk



Urs Hengartner
urs.hengartner@uwaterloo.ca



Leah Zhang-Kennedy
lzhangkennedy@uwaterloo.ca