VANCOUVER ISLAND UNIVERSITY

Smart Devices, Smarter Privacy

A Privacy-by-Design Workshop

Privacy Aware AI Research Team

Principle Investigator: Dr. Ajay K Shrestha
Funded by the Office of the Privacy Commissioner of Canada

RAs: Yulia Bobkova • Molly Campbell • Trevor De Clark • Mohamad Sheikho Al Jasem • Victor Olaleye • Saksham Sohal
Computer Science Department, Vancouver Island University (VIU), Canada

About Our Research

EMPOWERING YOUNG CANADIANS IN THE SMART DEVICE ERA

A Privacy-by-Design Research and Public Engagement Initiative

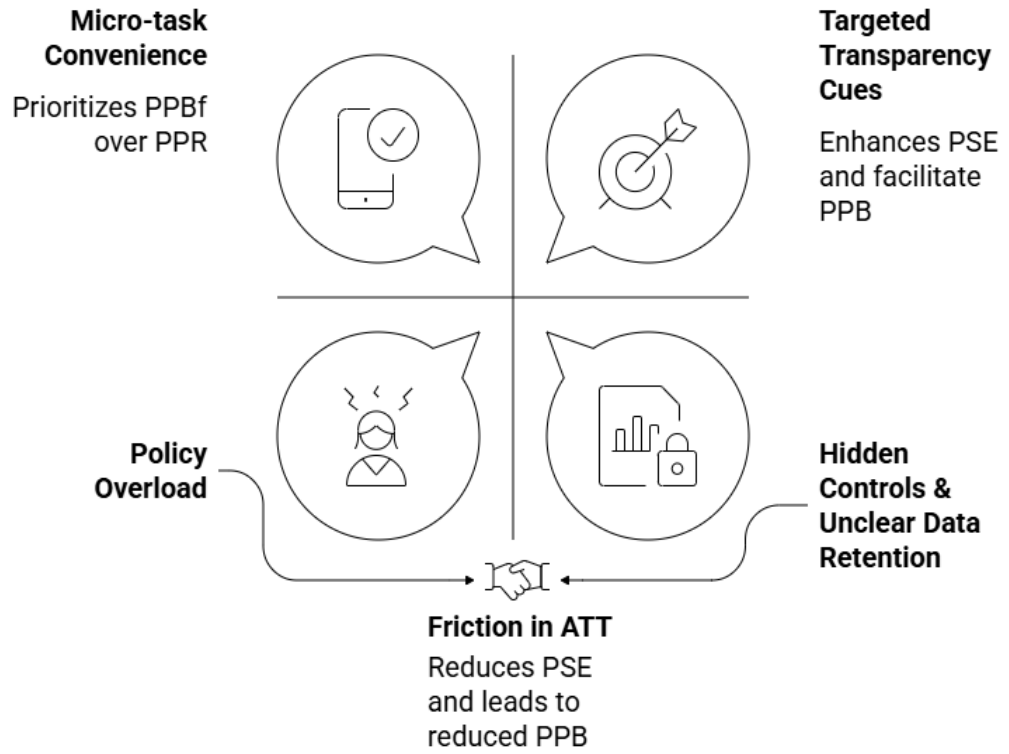
The overarching goal of this project is to empower youth (ages 16-24) with the knowledge and tools needed to safeguard their personal data in a rapidly evolving digital landscape, particularly in voice-activated AI apps. By emphasizing privacy-by-design principles and public engagement, we seek to foster an environment where responsible, privacy-centric AI practices become the norm.

RESEARCH QUESTIONS

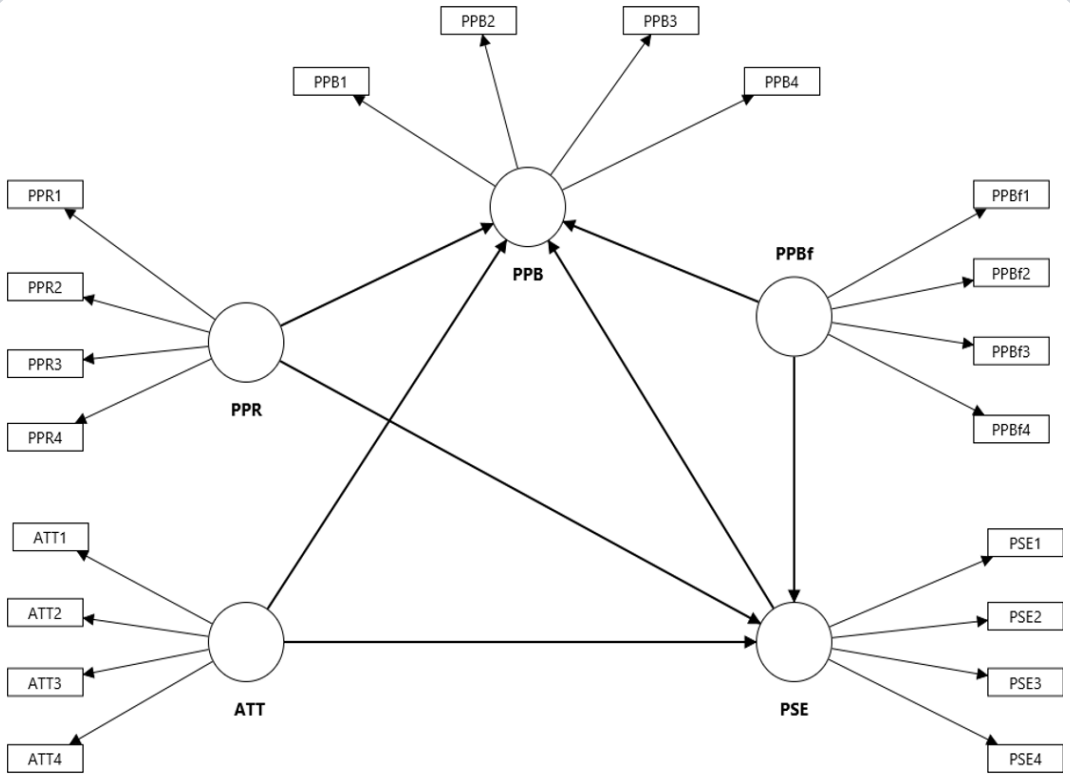
- Youth concerns around data collection and usage in voice-activated AI (e.g., Siri, Alexa).
- Influence of privacy risk, benefit perception, and transparency on trust and adoption.
- Current privacy controls used by youth and their impact on self-efficacy and protective behavior.
- Youth-suggested solutions (technical, policy, educational) to address privacy gaps and improve user control.

Focus Group Narratives

- **4 focus groups, N=22**
- **Key Takeaways:**
  - The problem is **wayfinding**, not awareness – Youth know privacy matters but can't find or understand controls
  - Policy overload, hidden settings, and deletion opacity destroy efficacy
  - Efficacy is **device-conditional** – Confident on phone, lost on speakers
  - Ambient listening anxiety – **"Always listening"** creates constant unease
  - Policy overload is real – Terms & conditions are long, unreadable, ignored
  - Deletion lacks **verification** – No confirmation data is actually gone
  - Physical strategies emerge from mistrust – Some disconnect mics internally; signals **profound control gap**
  - Convenience still matters – Micro-tasks and hands-busy use are valued
- **Design Suggestions:**
  - "Data nutrition labels" (plain language)
  - Unified privacy hub
  - Post-deletion receipts + auto-delete defaults
  - Micro-tutorials in-context
  - Hardware mute + clear status indicators



Results & Key Takeaways - Conceptual model (5 constructs) & PLS-SEM



Constructs

- **PPR:** perceived privacy risk
- **PPBf:** perceived privacy benefits
- **ATT:** algorithmic transparency & trust
- **PSE:** privacy self-efficacy
- **PPB:** privacy-protective behavior

PLS-SEM:

Path	Finding	Significance
PSE → PPB	Positive(β=0.37)	p<0.001
PPR → PPB	Positive (β=0.34)	p<0.001
PPBf → PPB	Negative (β=-0.13)	p<0.1
ATT → PPB	Not sig	p>0.1
ATT → PSE	Positive (β=0.43)	p<0.001
PPR → PSE	Not sig	p>0.1
PPBf → PSE	Positive (β=0.12)	p<0.1

Path	Effect	Finding
ATT → PSE → PPB	β=0.16	Full Mediation (p<0.001)
PPBf → PSE → PPB	β=0.045	Partial Mediation (p<0.05)
PPR→ PSE → PPB	Not sig	No Mediation

- **Key Takeaways:**
  - **PSE** is the strongest direct predictor of protective behavior
  - **The efficacy gap:** ATT has no direct effect on PPB; ATT works only through PSE. Trust in the system must build confidence first
  - **Privacy calculus:** Benefit directly discourages protective behavior, but benefits also boost efficacy; the trade-off is not binary
  - **Privacy paradox:** Concerned youth want to act (PPR → PPB), but risk doesn't build efficacy (PPR → PSE), concern without confidence = privacy fatigue

Results & Key Takeaways – Multigroup Analysis

Age-Differentiated Pathways:

- **Younger (16-18) vs Older (19-24)**
- **Mean Differences:**

Construct	Younger	Older
ATT	Higher	Lower
PPBf	Higher	Lower
PPR	Lower	Higher
PPB	Lower	Higher
PSE	No difference	

- **Pathway Differences:**
  - **ATT → PSE:** Younger β=0.36 vs Older β=0.57 (p<0.05)
  - All other paths are invariant across ages
- **Key Takeaways:**
  - **Core mechanism stable:** PSE → PPB drives behavior for ALL ages
  - **Age efficacy gap:** Younger youth have higher trust but it doesn't translate into confidence to act
  - Trust becomes actionable with age

Gender-Based Heterogeneity:

- **Male vs Female**
- **Mean Differences:**

Construct	Male	Female
PSE	Higher	Lower
PPBf	Higher	Lower
ATT, PPR, PPPB	No difference	

- **Pathway Differences:**
  - **PPR → PPB:** Female β=0.23 vs Male β=0.42 (p<0.1)
  - **ATT → PSE → PPB**: Female β=0.23 vs Male β=0.13 (p<0.1)
  - All other paths are invariant across gender
- **Non-Binary (Descriptive only – very small sample size):**
  - Lowest scoring ATT and PPBf means
  - Highest PPR mean for all groups
  - Distinct profile – needs further study
- **Key Takeaways**:
  - **Gender efficacy gap:** Males significantly more confident in privacy management
  - **Males:** Risk → Direct Action
  - **Females:** Trust → Efficacy → Action
  - PSE is gender-sensitive (failed measurement invariance)

Results & Key Takeaways – Clustering & Behavioral Indices

Privacy Profiles:

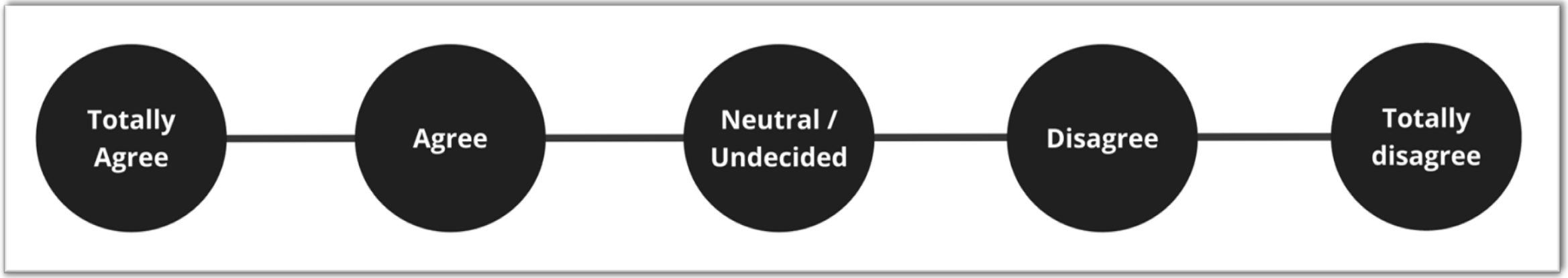
- **Two** distinct privacy profiles are identified using cluster analysis (N = 458)
- **Profile A: Concerned Skeptics**
  - High PPR
  - Low PPBf
  - Low ATT
  - Low PSE
  - Moderate PPB
- **Profile B: Confident Optimists**
  - Lower PPR
  - High PPBf
  - Higer ATT
  - Higer PSE
  - Moderate PPB

	Profile A	Profile B	Significance
Age	19.25 (older)	18.23 (younger)	p<0.001
User Frequency	Rarely	Often	p<0.001
Gender	No difference	No difference	n/a

Privacy Indices:

- **Risk-Benefit Tension Index (RBIT) =** zPPR-zPPBF
- **Control Acceptance Tension Index (CATI) =** avg(zPSE+zATT) – zPPBF
- **Control matters more than risk for predicting protective behavior**
  - CATI (β=0.21) stronger predictor than RBIT (β=0.07)
  - Aligns with prior finding: PSE is central driver
- **Frequent users = benefit-dominant + acceptance-leaning**
  - Daily users show the lowest RBIT and CATI
  - Suggests convenience may come at the cost of perceived control
- **Rare users = risk-dominant + control-dominant**
  - Rare users show the highest RBTI and CATI
- **Reframes the privacy paradox:**
  - Control dominant youth act, benefit-dominant youth don't
  - High concern + low action = risk-dominant BUT control-low

Activity 1 - Spectrogram



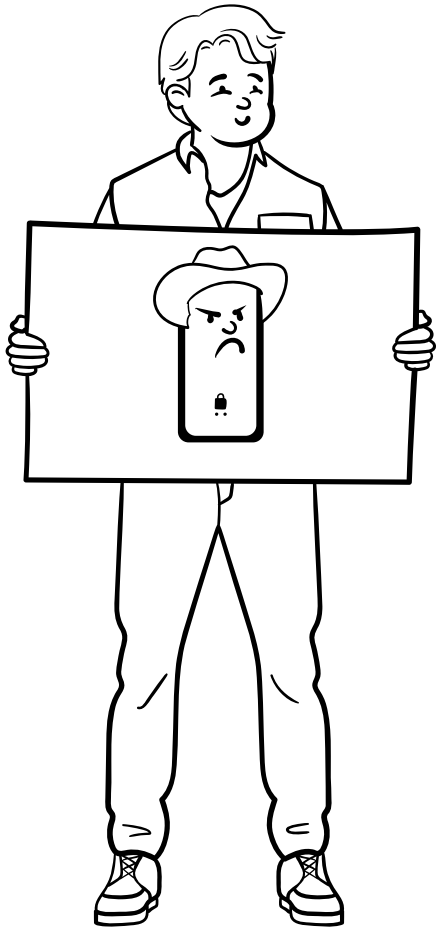
Activity 2 – Draw Your Assistant

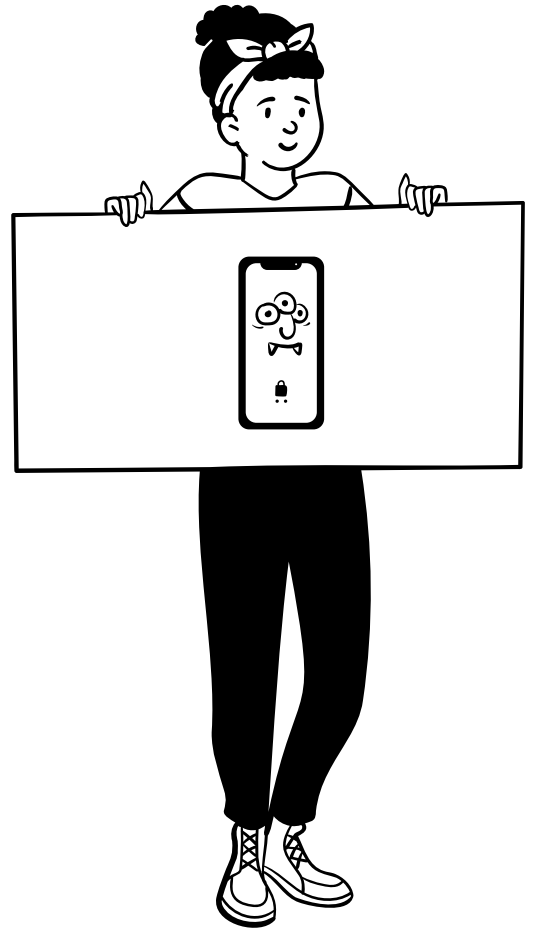
<u>Draw</u> your interpretation of your smart voice assistant

What does it say to you?

How does it behave?

Are they a helpful friend, a silent observer, or a creepy stranger?





Time for a Privacy Check-Up

Audit your own device with the provided template

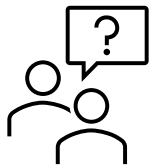
Activity 4 – Which Privacy Profile Are You?

The Concerned Skeptic

- **Core Mindset:** Highly skeptical of data collection practices, sees limited value in using smart voice assistants
- Perceives high privacy risks, low benefits of use
- Has low trust in the algorithms and in the companies that make these devices
- Lack self-confidence in their ability to manage privacy settings
- Exhibits moderate privacy protective behaviors

The Confident Optimist

- **Core Mindset:** Pragmatic users who recognize both the benefits and the risks but feel in control of their smart voice assistant use
- Perceives lower privacy risks, higher benefits of use
- Has higher trust in companies and their algorithms
- Have high self-confidence in their ability to manage privacy settings
- Exhibits moderate privacy protective behaviors



Q&A

Thank you!