SAFEGUARDING TOMORROW'S DATA LANDSCAPE:

Young digital citizens' perspectives on privacy within AI systems

This report is submitted in fulfillment of
the research project funded by
The Office of the Privacy Commissioner of Canada's (OPC)
Contributions Program

By

Dr. Ajay Shrestha
Principal Investigator
Professor, Computer Science Department
Privacy-Aware AI Research Team
Vancouver Island University
Nanaimo, BC, Canada

March 15, 2025

Contents

1. Executive Summary

This report provides comprehensive documentation of the *Safeguarding Tomorrow's Data Landscape* project, funded by the Office of the Privacy Commissioner of Canada's (OPC) Contributions Program. This research sought to investigate the privacy perceptions, concerns, and expectations of young digital citizens aged 16–19, alongside the perspectives of educators and parents, and AI developers and researchers. Throughout the study, the Principal Investigator (PI), leading the Privacy-Aware AI Research Team, delved into various models and theories of AI privacy to develop evidence-based guidelines and policy recommendations aimed at safeguarding youth data in AI-driven environments.

To establish a theoretical foundation, the study began with a systematic literature review on AI privacy, data governance, and youth digital rights. These insights informed the user studies, which included a robust data collection phase yielding 461 valid survey responses, supplemented by 12 interviews and 2 focus groups. The research employed both quantitative (Structural Equation Modeling, SEM) and qualitative (thematic analysis) methods to examine data ownership, parental data sharing, risk-benefit perception, transparency, and privacy awareness. The study developed the Privacy-Ethics Alignment in AI (PEA-AI) Model, a stakeholder-driven framework that defines privacy as a dynamic process shaped by negotiation, regulations, and AI design. Formulated using a grounded theory approach, the model aligns privacy governance with ethical considerations, emphasizing the need for adaptive, multi-stakeholder AI privacy management.

This study also highlights the dissemination strategies used to share findings and foster stakeholder engagement. Significant achievements include presentations at major IEEE conferences, where PI received recognition for research contributions. The project's outreach extended through a dedicated webinar, an in-person seminar on AI ethics and privacy, and a meet-up event, all of which facilitated interactive discussions, hands-on activities, and knowledge exchange among students, educators, and industry professionals. Additionally, findings were disseminated through social media channels, Medium articles, and mainstream media coverage, including features in the Nanaimo News Bulletin and The Jas Johal Show on CKNW Radio. The PI also received an invitation as an invited speaker at the ACM Seventh International Conference on Blockchain Technology and Applications (ICBTA) in Xi'an, China, reflecting the growing interest in decentralized AI models and privacy solutions.

Concluding with proposed guidelines and policy recommendations, this report offers clear strategies for youths, educators, policymakers, AI developers, and parents to enhance youth privacy protections. The final chapters explore the next steps, including the need for continuous guideline refinement, potential legislative updates, and expanded research on emerging AI applications. By documenting the entire research journey, this report underscores how the study's outcomes support the OPC's broader mandate to protect personal information and foster a safer digital environment for Canada's youth.

2. Introduction

This project was conceived in response to the rapid adoption of AI technologies across educational, social media, and entertainment platforms where young people are often the primary users. The lack of robust privacy protocols and transparent data practices in these AI systems raises significant ethical and regulatory concerns, making it crucial to investigate how young users interact with AI-driven services and perceive data governance. Furthermore, educators and parents play pivotal roles in shaping responsible digital citizenship, while AI professionals' perspectives on balancing innovation with privacy offer critical insights into potential policy pathways.

2.1 Project Scope and Relevance

Young digital citizens navigate a complex AI ecosystem, from personalized learning applications to social media recommendation algorithms. This research was initiated to address a pressing question: "How can we better protect the privacy of young digital citizens within AI systems while maintaining the benefits these technologies offer?" Building on frameworks like PIPEDA[1] (Personal Information Protection and Electronic Documents Act) and international guidelines, the study aimed to contextualize the unique vulnerabilities of youths who often lack the experience or resources to make fully informed decisions about their personal data.

Several articles and announcements spotlighted the urgency of this project. For instance, the Nanaimo News Bulletin piece "VIU researcher studying youth opinions on AI[2]" underscored the necessity of this research in local educational contexts. Medium articles such as "Empowering the Next Generation: Safeguarding Young Digital Citizens' Privacy in AI Systems[3]" and "Connecting with the Community at VIU Fest: A Step Forward for AI Privacy[4]" further emphasized the breadth of public interest and the community's willingness to engage with privacy issues.

2.2 Overview

This research began with a systematic literature review guided by the PRISMA[5] methodology. Starting with over 2,000 publications, the screening process refined the pool to 108 relevant studies, focusing on how young digital citizens perceive and manage privacy in AI contexts, including social media platforms, educational technology, gaming systems, and recommendation algorithms. This review underscored significant gaps in youth-centric privacy research, particularly concerning data ownership, parental data sharing, perceived risks and benefits, trust and transparency, and education and awareness [1].

[1] https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/strengthening-privacy-digital-age

[2] https://www.nanaimobulletin.com/home/viu-researcher-studying-youth-opinions-on-ai-7521334

[3]https://medium.com/@PrivaLab/empowering-the-next-generation-safeguarding-young-digital-citizens-privacy-in-ai-systems-ae29cb22f4f5

[4] https://medium.com/@PrivaLab/connecting-with-the-community-at-viu-fest-a-step-forward-for-ai-privacy-be24879e5ac1

[5] https://www.prisma-statement.org/

Following ethics approval from the VIU Research Ethics Board (REB), the team conducted surveys, interviews, and focus groups to gather empirical data from key stakeholder groups: young digital citizens, parents/educators, and AI professionals. The research employed two foundational theories—Privacy Calculus Model (PCM) [2], [3] and Communication Privacy Management (CPM) [4], [5]—to examine how individuals weigh potential risks against perceived benefits when deciding whether to disclose personal information, and how they establish and negotiate privacy boundaries within AI-driven environments.

Building on these theoretical underpinnings and real-world insights, the study developed a novel model, termed the Privacy-Ethics Alignment in AI (PEA-AI) Model [6], through a grounded theory approach [7]. This model integrates stakeholder perspectives to propose an adaptive, negotiation-based framework for ethical AI governance. By situating youth experiences at the forefront, the PEA-AI Model aims to address existing research gaps and guide the development of AI systems and policies that effectively safeguard young users' privacy.

2.3 Research Questions and Objectives

This section outlines the guiding inquiries and corresponding aims of the study, focusing on how young digital citizens, alongside educators, parents, and AI professionals, shape our understanding of privacy in AI systems.

Research Questions

- **Research Question 1**: How do young digital citizens (aged 16–19) perceive privacy in the context of AI systems?
- **Research Question 2**: What are the primary privacy concerns and expectations among young digital citizens (aged 16–19) when interacting with AI-driven platforms?
- **Research Question 3**: How do educators, parents, and AI professionals perceive their roles in supporting or regulating AI privacy for young people?
- **Research Question 4**: What guidelines and policy recommendations can be formulated to protect youth data effectively, ensuring transparent, ethical AI system use?

In pursuit of these questions, this project set forth the following objectives:

- Identify key privacy concerns through empirical data collection (surveys, interviews, focus groups).
- Develop a rigorous analytical framework using the Structural Equation Modeling Technique and qualitative thematic analysis to elucidate core themes.
- Understand how parents, educators, and AI professionals perceive their roles in safeguarding youth privacy.
- Propose actionable guidelines grounded in evidence-based best practices and stakeholder feedback.
- Disseminate findings via academic publications, conference presentations, social media, and community engagement events.

This study addresses a critical gap in AI ethics literature by centering on youth experiences and perspectives. The outcomes not only reinforce the OPC’s mandate but also provide valuable input for policymakers, educators, and industry stakeholders seeking to design AI applications that respect personal data rights. Ultimately, the research contributes to a growing body of knowledge on ethical AI, informing both national policy dialogues and international conversations on children’s digital rights.

3. Research Design, Data Collection and Methodology

The study received ethics approval from the Vancouver Island University Research Ethics Board (VIU-REB). The approval reference number #103116 was given for behavioral application/amendment forms, consent forms, interview and focus group scripts, and questionnaires. An initial pilot study was conducted with 6 participants, including members of the empirical research specialists from the University of Saskatchewan and Vancouver Island University. The pilot study aimed to evaluate the feasibility and duration of the research approach while refining the study design. Participants offered general feedback on the questionnaire, which guided modification and restructuring of the final survey. The revised research model was then tested by gathering survey data. Survey data was collected by recruiting participants through flyers, personal networks, emails, and social networking sites, LinkedIn and Reddit. To reach our targeted youth demographic, the research team reached out to several Vancouver Island school districts for their assistance in distributing the survey to their high-school students. Participation in the study was entirely voluntary and did not receive any form of compensation. The participants had to read and accept a consent form before starting the questionnaire. By submitting the consent form participants were indicating that they understood the conditions of participating in the study as outlined in the consent form. The research team conducted online surveys through Microsoft forms by requesting each participant to respond to the questionnaire based on the three designated demographics: AI Researchers and Developers, Parents and Teachers, and Young Digital Citizens (aged 16-19).

In addition to the survey questionnaires, the research team also conducted interviews and focus groups with AI professionals, parents, and educators. One section of the questionnaire invited participants to provide their email addresses if they were interested in participating in interviews and/or focus groups. After contacting those who consented, the team conducted 12 interviews and 2 focus groups: one with 4 AI professionals and another with 5 parents and/or educators. Before the interviews and focus groups, all participants were provided with a consent form to review and accept. Interviews and focus groups were conducted and transcribed using Microsoft Teams, with participants instructed to keep their videos off to ensure anonymity.

The survey instruments were adapted from constructs validated in prior studies [2], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20]. The instruments consist of 3 indicators for Data Ownership and Control (DOC), 2 indicators for Parental Data Sharing (PDS), 4 indicators for Perceived Risk and Benefits (PRB), 3 indicators for Trust and Transparency (TT), 3 indicators for Education and Awareness (EA), and 3 open-ended discussion questions. The items (questions) corresponding to these constructs, along with their definitions, are outlined in Table I.

TABLE I. Constructs and items

Construct	Definition	Items
Data Ownership and Control (DOC)	It is the degree to which young people have control over their personal data and engage in discussions about privacy.	doc1: Importance of users having control over their personal data. (Data Control Importance) doc2: Frequency of considering user data control in work. (Perceived Data Control) doc3: Feasibility/comfortability of implementing data control mechanisms. (Comfort Data Sharing)
Parental Data Sharing (PDS)	It is the degree to which parents exercise their rights to share children's data and consider the implications of doing so.	pds1: Handling data shared by parents on behalf of children. (Parental Data Sharing) pds2: Importance of obtaining consent from young users. (Parental Data Rights)
Perceived Risks and Benefits (PRB)	It is the degree to which individuals perceive risks, ethical concerns, and benefits related to the use of personal data by AI systems.	prb1: Concern about ethical/privacy implications. (AI Privacy Concerns) prb2: Significance of benefits in justifying data use. (Perceived Data Benefits) Open-Ended Question: Primary risks associated with personal data use. Open-Ended Question: Benefits AI systems provide by using personal data.
Transparency and Trust (TT)	It is the degree to which transparency in data usage influences trust in AI systems.	tt1: Importance of transparency about data usage. (Data Usage Transparency) tt2: Perception of transparency in current AI systems. (Transparency Perception) tt3: Belief that increasing transparency improves user trust. (System Data Trust)
Education and Awareness (EA)	It is the degree to which stakeholders are informed about privacy and ethical issues associated with AI.	ea1: Knowledge about privacy issues related to AI systems. (Privacy Protection Knowledge) ea2: Belief that users receive adequate training on privacy. (Digital Privacy Education) ea3: Importance of being educated on privacy and ethical issues/ Adequacy of privacy information. (AI Privacy Awareness)

Responses to the items were measured on a 5-point Likert scale, with most items used for quantitative analysis. Notably, to ensure consistency in outcomes, we reversed the scale for items in PRB for AI professionals and swapped items 1 and 2 in PDS for young digital citizens to algin contextually with the items for the other demographics. For qualitative analysis, we used open-ended questions, two indicators from PRB, interview responses, and focus group discussions.

We use the following naming conventions for qualitative responses. We label survey participants as (S-YDC #X) for young digital citizens, (S-PE #X) for parents and educators, and (S-AIP #X) for AI Professionals. We refer to interview participants as (I-[Role] #X), specifying their role, such as I-Parent #1 or I-Educator #2. For focus group participants, we use a group identifier and role, such as (FG1-Educator #3).

This study used a mixed-methods approach to capture a nuanced understanding of youth AI privacy concerns. The methodology combined quantitative surveys, and qualitative open-ended questions and interviews/focus groups, ensuring robust triangulation of data sources.

3.1 Participant Recruitment

Data collection targeted three primary groups:

- Young Digital Citizens (16–19): The project collaborated with school districts in Sooke (SD62), Nanaimo and Ladysmith (SD68), and Cowichan (SD79), alongside VIU campus events such as VIU Fest. Social media announcements and word-of-mouth referrals further expanded youth participation.
- Educators/Parents: Emails were sent through school districts, and VIU educator circles, inviting them to share perspectives on AI's role in classrooms and homes.
- AI Professionals: The research team reached out to IEEE members (15th IEEE Annual Information Technology, Electronics and Mobile Communication Conference–IEMCON participants and technical program committee), AI industry meetups, LinkedIn communities, and academic networks, ensuring representation from AI developers, researchers, and practitioners.

3.2 Data Collection Timeline

- **Initial Period**: The original data collection window concluded on October 31, 2024. However, due to slow district approvals, the project requested and received an extension from the OPC and VIU's Research Ethics Board (REB) until December 20, 2024, ensuring broader youth involvement.
- **School District Approvals**: Approvals were obtained from school districts in Sooke (SD62), Nanaimo and Ladysmith (SD68), and Cowichan (SD79), which allowed for direct engagement with high school students under supervised conditions. Outreach to other districts was undertaken, though only the above granted timely approval.

3.3 Final Dataset

Out of 482 participants, 461 completed the survey questionnaire: 176 young digital citizens (aged 16–19), 132 parents and/or educators, and 153 AI professionals. After data cleaning, we retained 127 valid responses from educators and/or parents, 146 from AI professionals, and 151 from young digital citizens for analysis. Of the 127 valid responses from educators and/or parents, 54 identified as parents, 46 identified as educators, and 28 identified as both. Among the 146 valid responses from AI professionals, 46 identified as AI developers, 98 as AI researchers, and 2 as both. We conducted 12 interviews, 9 interviewees identified as a parent and/or educator, and 3 identified as

AI professionals. We also conducted 2 focus groups, 4 participants identified as AI professionals, and 5 as parents and/or educators. Table II highlights the characteristics of the demographics of the participants.

TABLE II. Participants' Demographics

Respondents' characteristics	**Percentage**			**Number of participants (n)**		
	Survey	**Interviews**	**Focus Groups**	**Survey**	**Interviews**	**Focus Groups**
Young Digital Citizens	35.6%	0.0%	0.0%	151	0	0
Parents	12.7%	8.3%	11.1%	54	1	1
Educators	10.8%	41.7%	33.3%	46	5	3
Both Parent and Educator	6.4%	25.0%	11.1%	27	3	1
AI Developers	10.8%	16.7%	33.3%	46	2	3
AI Researchers	23.1%	8.3%	11.1%	98	1	1
Both AI Developers and Researcher	0.5%	0.0%	0.0%	2	0	0

3.4 Data Management and Security

This research rigorously adhered to privacy and ethical guidelines:

- **Secure Storage:** All raw and cleaned data were securely stored on MS OneDrive with restricted access to the Principal Investigator and research assistants.
- **Deletion from MS Forms:** In compliance with ethical protocols, survey data was removed from MS Forms on January 20, 2025, exactly one-month post-collection closure.
- **Ethical Considerations:** Informed consent procedures, confidentiality assurances, and secure handling of personal information were rigorously upheld. The VIU REB monitored participant consent processes and assured that confidentiality was maintained throughout data handling.

3.5 Public Availability of Survey Dataset

As a publicly funded research project, ensuring transparency and open access is a key priority. To support further research and public engagement, the cleaned and anonymized survey dataset for each stakeholder group has been made publicly available in the project's GitHub repository[6]. This dataset has been processed to remove personally identifiable information while preserving the integrity of the responses for meaningful analysis. By providing open access, the project aims to contribute to ongoing discussions on AI privacy, facilitate collaborative research, and support evidence-based policymaking.

[6] https://github.com/csci-viu/privacy-aware-ai-for-youth

4. Data Analysis and Key Findings

The research team employed both quantitative (Descriptive Statistics and SEM) and qualitative (thematic) methods to interpret the collected data, ensuring a multidimensional understanding of youth AI privacy needs, and to uncover critical privacy negotiation points and demonstrate how multi-stakeholder discourse shapes privacy governance.

4.1 Descriptive Statistics

The quantitative survey used a 5-point Likert scale to compare mean responses across five key constructs: Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA). The mean scores for each construct varied across three key demographics-young digital citizens, parents and/or educators, and AI professionals. The results are visually represented in Fig. 1, where the overall mean for each construct is calculated by combining all items within that construct.

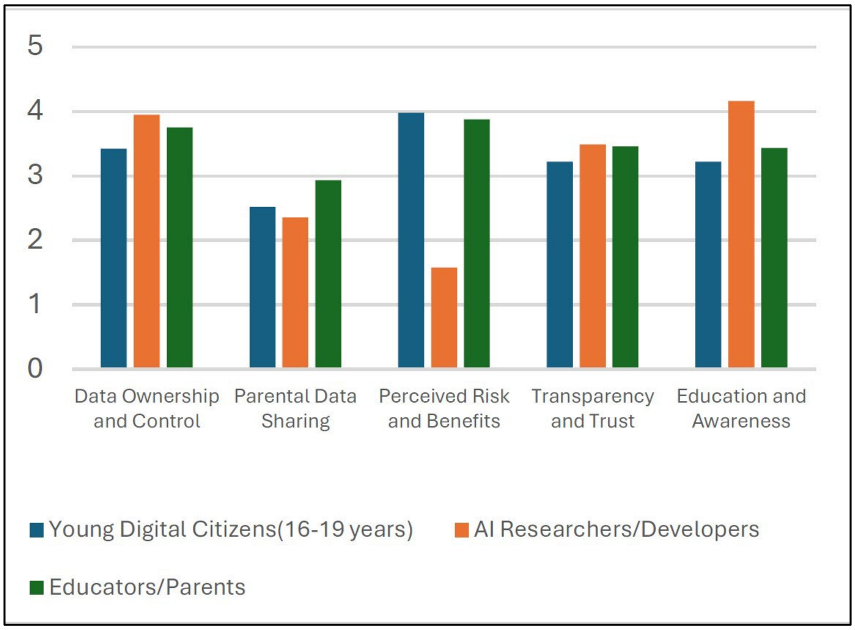

Fig. 1. Means across constructs and demographics.

AI developers and researchers rated DOC highest (3.95), reflecting their focus on autonomy and control over personal data, followed by educators and parents (3.75) and young digital citizens (3.42), who may feel less equipped to assert ownership. Low PDS scores across groups (2.36 for AI professionals, 2.94 for educators/parents, and 2.52 for youth) indicated hesitancy in data-sharing practices, highlighting a general preference for restricting parental involvement in data disclosure.

Perceived Risks and Benefits (PRB) showed the most variation, with young digital citizens rating it highest at 3.98, indicating their recognition of the dual nature of AI's advantages and vulnerabilities. Educators and parents followed closely at 3.88, demonstrating concern for the ethical trade-offs in data use. Interestingly, AI developers and researchers rated PRB significantly lower at 1.58, which may stem from their focus on technical feasibility over user-centric risks and benefits. This divergence underscores the importance of bridging technical and ethical considerations in AI development.

Transparency and Trust (TT) and Education and Awareness (EA) scores further emphasized the disparities between groups. AI developers and researchers rated EA highest (4.16), signaling their prioritization of digital literacy and privacy safeguards, whereas educators and parents scored 3.43, reflecting their role in promoting awareness. Youth scored lower at 3.22, revealing a gap in understanding and confidence. TT followed a similar pattern, with AI professionals (3.49) and educators/parents (3.46) scoring higher than youth (3.22), underscoring the importance of fostering trust and transparency to empower young users in navigating AI systems. These results highlight the need for targeted interventions to address trust, awareness, and data-sharing disparities across stakeholders.

Additionally, Fig. 2 (heatmap) presents each item's mean score across all stakeholder groups individually. By examining mean scores across items, key differences emerge in the conceptualization of data control, parental data sharing, perceived risks and benefits, transparency, trust, and education.

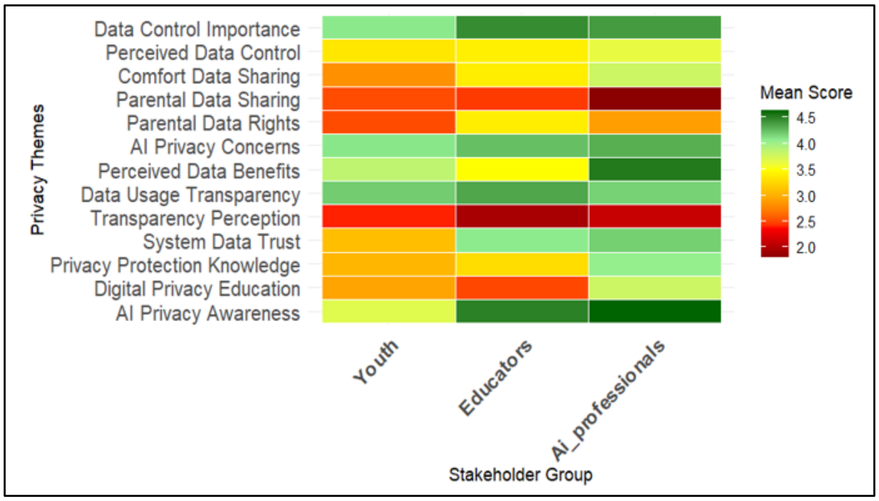

Fig. 2. Heatmap analysis

1) Data Ownership and Control (DOC)

a) Data Control Importance: Parents/Educators rated this highest (4.46), followed by AI Professionals (4.39) and Youth (4.08). This suggests that adult stakeholders, especially educators and researchers, strongly advocate for user control over personal data, reinforcing its role in ethical AI development.

b) Perceived Data Control: AI Professionals (3.64) reported feeling more in control over their data compared to Parents/Educators (3.40) and Youth (3.35). The relatively lower score among youth suggests a potential gap in privacy self-efficacy, necessitating better user-centric privacy mechanisms.

c) Comfort with Data Sharing: AI Professionals (3.79) displayed the highest comfort in sharing personal data, followed by Parents/Educators (3.39), with Youth reporting the lowest comfort (2.`83). This reflects a generational divide in risk perception, with youth demonstrating greater apprehension towards personal data disclosure.

2) Parental Data Sharing (PDS)

a) Parental Data Sharing Practices: AI Professionals reported the lowest support for parental data sharing (1.81), followed by Parents/Educators (2.46), and Youth (2.52). These relatively low scores indicate widespread concerns about the appropriateness of parental involvement in youth data decisions.
b) Parental Data Rights: Parents/Educators (3.39) rated parental data rights the highest, while AI Professionals (2.90) and Youth (2.51) expressed lower confidence in this construct. Notably, AI professionals, favored youth consent mechanisms, prioritizing autonomy over parental governance in data-related decisions.

3) Perceived Risks and Benefits (PRB)

a) AI Privacy Concerns: All three groups expressed strong privacy concerns, with AI Professionals scoring the highest (4.31), followed by Parents/Educators (4.25) and Youth (4.09). This consensus highlights the universal recognition of ethical challenges posed by AI data governance.
b) Perceived Data Benefits: AI Professionals (4.53) rated data benefits significantly higher than both Youth (3.86) and Parents/Educators (3.50). These findings suggest that while AI professionals see tangible advantages in data-driven AI advancements, youth and educators remain more cautious, reflecting a trust gap in AI benefit perception.

4) Transparency and Trust (TT)

a) Data Usage Transparency: Transparency was considered highly important across all stakeholder groups, with Parents/Educators scoring highest (4.34), followed by Youth (4.19) and AI Professionals (4.17). This reinforces the demand for increased transparency mechanisms in AI governance.
b) Transparency Perception: Despite valuing transparency, stakeholders perceived existing AI transparency measures as insufficient. Parents/Educators rated transparency perception lowest (1.96), followed by AI Professionals (2.11), and Youth (2.41). These results indicate a strong disparity between their expectations and the current implementation of transparency in AI systems.
c) System Data Trust: AI Professionals (4.18), followed by Parents/Educators (4.07), exhibited relatively higher trust in AI systems, while Youth expressed significantly lower trust (3.09). These findings suggest that youth are more skeptical of AI governance practices, reinforcing the necessity of improved explainability measures.

5) Education and Awareness (EA)

a) Privacy Protection Knowledge: AI Professionals reported the highest levels of privacy knowledge (4.04), followed by Parents/Educators (3.29) and Youth (3.04). The significant gap between professionals and youth suggests an urgent need for targeted AI privacy education initiatives.
b) Digital Privacy Education: AI Professionals rated privacy education substantially higher (3.79) compared to Youth (2.93) and Parents/Educators (2.50). These results highlight a potential divide in AI literacy, where non-technical stakeholders may lack the resources to fully understand privacy frameworks.
c) AI Privacy Awareness: All groups strongly agreed on the importance of AI privacy education, with AI Professionals rating it highest (4.63), followed by Parents/Educators (4.50) and Youth (3.68). The widespread alignment in this area suggests broad recognition of the need for continuous privacy education programs.

4.2 Structural Equation Modeling (SEM)

The research team employed a partial least squares structural equation modeling (PLS-SEM) approach using SmartPLS software [21]. PLS-SEM is a widely used method for estimating path coefficients in structural models and is recognized across numerous studies [22], [23]. As recommended by [24], SEM involves testing measurement models—incorporating exploratory factor analysis, internal consistency, convergent validity, and Dillon-Goldstein's rho—along with evaluating the structural model through regression analysis. The path-weighting structural model scheme in SmartPLS was applied to maximize the R^2 values for dependent latent variables.

Additionally, the analysis incorporated a nonparametric bootstrapping procedure. Bootstrapping, a resampling technique, generates an empirical sampling distribution by repeatedly drawing samples with replacements from the original dataset. For this study, 5,000 subsamples were generated, and a two-tailed test was conducted at a significance level of 0.1.

The structural model was analyzed by examining the coefficients of determination (R^2), path coefficients (β), and corresponding p-values. The R^2 values indicate the variance explained by the antecedent constructs, while the β values measure the strength of relationships between constructs. The p-values assess statistical significance. According to Chin's guidelines [13], [25], a β value of at least 0.2 is considered relevant. Statistical significance is categorized as somewhat significant (*p) for p-values < 0.1, quite significant (**p) for p-values < 0.01, and highly significant (***p) for p-values < 0.001 [13], [25].

Figures 3–5 present the structural models for the three stakeholder groups, illustrating the causal relationships (direct paths) among Data Ownership and Control (DOC), Education and Awareness (EA), Parental Data Sharing (PDS), Perceived Risk and Benefit (PRB), and Trust and Transparency (TT). The model evaluates direct, indirect, and total effects among these constructs. The full analysis is detailed in the IEEE Access paper, with a preprint available online [3].

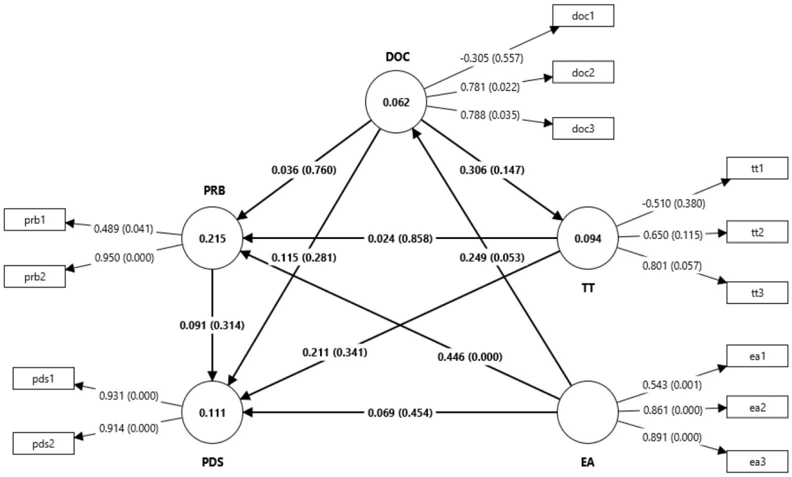

Fig. 3. Structural model for young digital citizen

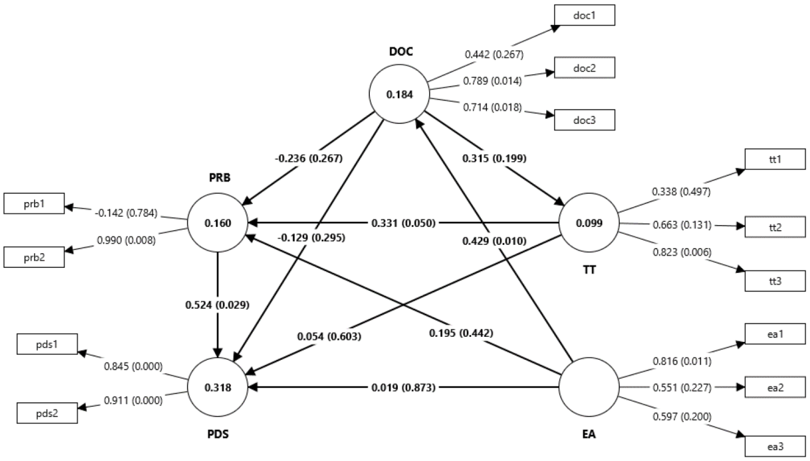

Fig. 4. Structural model for parents/educators

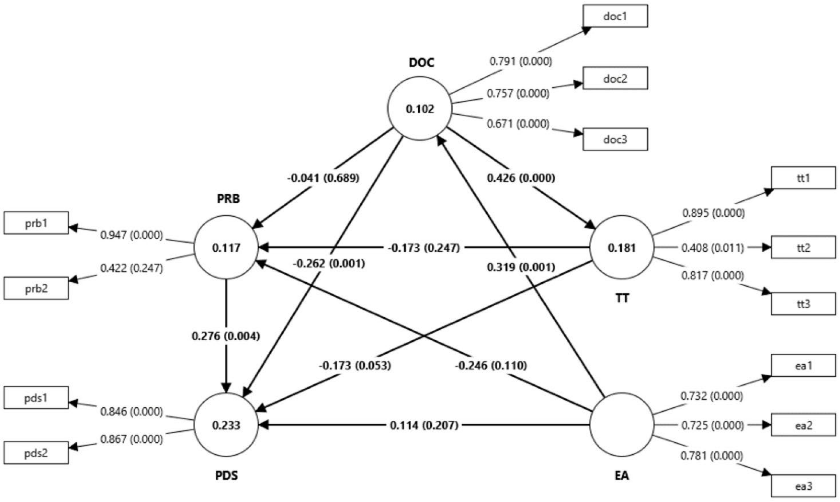

Fig. 5. Structural model for AI professionals

Summary of PLS-SEM Model Interpretations:

1) *Model 1: Young Digital Citizens*

    a) Education and Awareness (EA) strongly influences Perceived Risks and Benefits (PRB) (β = 0.446, p < 0.001), indicating that youth with higher awareness better understand AI-related risks and benefits.

    b) Data Ownership and Control (DOC) does not significantly impact Trust and Transparency (TT) (β = 0.306, p > 0.1), suggesting that youth do not strongly link personal control over data with trust in AI.

    c) Perceived Risks and Benefits (PRB) does not significantly influence Parental Data Sharing (PDS) (β = 0.091, p > 0.1), meaning concerns about AI risks do not directly affect their willingness to share data.

    d) Education and Awareness (EA) positively affects Data Ownership and Control (DOC) (β = 0.249, p < 0.1), suggesting that greater awareness encourages youth to assert more control over their data.

    e) Transparency and Trust (TT) does not significantly impact Perceived Risks and Benefits (PRB) (β = 0.024, p > 0.1), indicating that trust in AI systems does not necessarily translate to a change in how youth perceive risks and benefits.

Key Insight: Youth rely on education to shape their understanding of AI risks, but they do not strongly associate transparency or data control with trust in AI. Their willingness to share data remains unaffected by risk perception.

2) *Model 2: Parents and Educators*

    a) Perceived Risks and Benefits (PRB) negatively impacts Parental Data Sharing (PDS) (β = 0.524, p < 0.1), showing that higher concerns about AI risks lead to lower willingness to share data.

    b) Transparency and Trust (TT) positively influences Perceived Risks and Benefits (PRB) (β = 0.331, p < 0.1), suggesting that greater transparency helps balance concerns about AI risks and benefits.

    c) Education and Awareness (EA) strengthens Data Ownership and Control (DOC) (β = 0.429, p < 0.1), indicating that higher awareness leads parents and educators to prefer more control over data.

    d) Education and Awareness (EA) does not significantly affect Parental Data Sharing (PDS) (β = 0.019, p > 0.1), implying that awareness does not directly change parents' willingness to share data.

    e) Data Ownership and Control (DOC) does not directly influence Parental Data Sharing (PDS) (β = -0.129, p > 0.1), suggesting that control over data is not a determining factor in parental data-sharing decisions.

Key Insight: Parents and educators are more cautious about data sharing when they perceive higher risks. Transparency helps balance concerns, while education enhances data control preferences but does not directly change data-sharing behavior.

3) *Model 3: AI Professionals*

a) Data Ownership and Control (DOC) positively influences Trust and Transparency (TT) (β = 0.426, p < 0.001), indicating that AI professionals see strong user control as a key factor in fostering trust in AI.
b) Perceived Risks and Benefits (PRB) positively affects Parental Data Sharing (PDS) (β = 0.276, p < 0.01), suggesting that AI professionals factor ethical considerations into data-sharing decisions.
c) Data Ownership and Control (DOC) negatively impacts Parental Data Sharing (PDS) (β = -0.262, p < 0.01), meaning those who strongly support data control are less likely to endorse broad parental data-sharing policies.
d) Education and Awareness (EA) enhances Data Ownership and Control (DOC) (β = 0.319, p < 0.01), reinforcing the idea that education leads to stronger preferences for data control.
e) Transparency and Trust (TT) has a moderate negative effect on Parental Data Sharing (PDS) (β = -0.173, p < 0.1), suggesting that as AI systems become more transparent, professionals may become more cautious about data sharing.
f) Perceived Risks and Benefits (PRB) does not significantly impact Trust and Transparency (TT) (β = -0.173, p > 0.1), indicating that risk perception does not strongly shape AI professionals' trust in AI.

Key Insight: AI professionals view data control as essential for trust in AI. While they acknowledge ethical considerations in data sharing, they tend to oppose broad parental data-sharing policies. Transparency makes them more cautious, and risk perception does not strongly influence their trust in AI.

Collectively, these findings underscore the context-specific drivers of AI-related behaviors and attitudes across different stakeholder groups, suggesting that interventions and policies should be tailored to each group's unique perspectives on trust, risk, and data control.

4.3 Qualitative Findings (Surveys, Interviews and Focus Groups)

In addition to the quantitative analysis, qualitative data was collected through open-ended survey responses, interviews, and focus groups to capture stakeholder perspectives on privacy concerns in AI systems.

1) *Key Privacy Concerns*

Collectively, concerns such as loss of data control, third-party sharing, excessive data collection, automated decisions, biased outcomes, surveillance, cybersecurity risks, profiling, over-personalization, and limited consent mechanisms emerged across different groups, though the prominence of each concern varied by stakeholder.

a) **Young Digital Citizens:** They were particularly concerned about losing control over their personal information, unauthorized data sales, and the risk of AI profiling their behaviors and preferences. Many youth respondents feared being tracked, manipulated, or profiled based on their online interactions. One respondent stated, “My data could be sold without my knowing who it’s going to” (S-YDC #107). Others worried about AI-enabled surveillance and identity risks, such as “I feel uncomfortable knowing AI can recognize my face in public places” (S-YDC #93).

b) **Educators/Parents:** They expressed similar concerns but focused more on the lack of awareness and informed decision-making among youth regarding data sharing. One parent emphasized, “Many children and adolescents will use AI without considering their own privacy… there is a lack of education regarding these risks” (S-PE #40). Cybersecurity risks were also a major concern, with respondents worried about data breaches and AI systems exposing sensitive student information.

c) **AI Professionals:** AI Professionals echoed these concerns but also highlighted the long-term risks of data retention and unintended information exposure. One AI researcher noted, “Once data goes into an AI system, it’s tough to know where it ends up or who else can see it” (S-AIP #45). Several professionals mentioned the risk of AI models inadvertently leaking private data, emphasizing that current privacy safeguards remain inadequate.

2) *Perceived Benefits of AI Data Usage*

Despite privacy concerns, all groups acknowledged the potential benefits of AI systems using personal data, particularly in education and personalized services.

a) Young Digital Citizens mentioned that AI helps with homework, learning, and content recommendations, if their personal data is not excessively collected. One youth explained, “I use AI tools for homework but try not to share personal stuff” (S-YDC #15).

b) Parents and Educators highlighted AI’s role in personalized learning, accessibility, and administrative efficiency. Some educators noted that AI tools can tailor lessons to students’ learning styles while ensuring privacy through anonymized data.

c) AI Professionals saw broader advantages, including optimized service delivery and efficiency in software development. One developer stated, “AI can analyze personal data to provide highly tailored services” (FG2-Developer #4). However, professionals also stressed the need for privacy-conscious AI development.

3) *Proposed Privacy Safeguards*

All groups emphasized the need for greater transparency, stronger privacy protections, and digital literacy initiatives.

a) Young Digital Citizens called for clearer privacy settings, real-time consent mechanisms, and simplified privacy policies. Some suggested, “Make privacy options super clear and right in front when I install an app” (S-YDC #67). Others advocated for global privacy standards and educational programs on digital privacy.

b) Parents and Educators focused on stricter regulations, youth-centric privacy laws, and educational initiatives. One parent recommended, “We need something more like the EU GDPR + AI Act to protect youth data” (S-PE #76). Many respondents supported age-based privacy controls and school-led AI literacy programs.

c) AI Professionals suggested technical privacy solutions, including data anonymization, encryption, federated learning, and differential privacy. A researcher emphasized, “To enhance privacy, AI should prioritize data minimization, anonymization, and explainability” (S-AIP #7). Unlike other groups, AI professionals were less focused on regulations and more interested in technical safeguards and user controls.

In conclusion, these qualitative findings underscore the need for multi-faceted privacy strategies in AI systems, balancing data utility with user protection. While youth prioritize platform-level privacy controls, parents and educators stress regulations and education, and AI professionals advocate for technical safeguards. The full qualitative analysis is available in the manuscript (submitted for review) [3].

4.4 Key Concerns Identified

The analysis of both quantitative and qualitative findings highlights critical privacy concerns in AI systems, particularly for young digital citizens. This section consolidates the main issues that require attention for policy development and intervention strategies.

1) Data Ownership and Control Uncertainty

Many participants, especially in educational settings, expressed confusion about who ultimately owns and controls the data collected by AI systems. Young users feel disconnected from decision-making, while parents and educators struggle to find clear guidelines on data governance. AI professionals acknowledge this gap but focus on technical solutions that are not always accessible to end-users.

2) Concerns About Parental Data Sharing

Parents worry about how much of their child’s data is shared with external organizations and feel uninformed about consent mechanisms. They emphasized the need for clearer policies and opt-in/opt-out controls to ensure they can make informed decisions about their children’s digital footprints.

3) Balancing AI Benefits and Privacy Risks

While stakeholders recognize AI’s potential for enhancing education and providing personalized services, concerns about data misuse, security breaches, and unethical data practices remain. Many participants felt that the benefits of AI should not come at the cost of personal privacy, calling for privacy-conscious AI designs that limit unnecessary data collection.

4) Lack of Transparency in AI Systems

There was universal agreement on the need for greater transparency in AI-driven platforms. Users want clear disclosures on what data is collected, how it is used, and how algorithmic decisions are made. Youth, in particular, struggled to trust AI systems due to the complexity and vagueness of privacy policies.

5) Insufficient Privacy Education and Awareness

Across all groups, participants noted a lack of accessible privacy education resources.

a) Youth feel unprepared to navigate AI privacy settings and understand their rights.
b) Parents and educators lack structured guidance to teach privacy-conscious behavior.
c) AI professionals recognize the need for better public engagement on AI privacy risks and solutions.

6) Weak Governance and Accountability in AI Privacy

While all groups agree on the need for stronger privacy protections, their perspectives differ:

a) Parents and educators seek clear regulations and stronger accountability measures.
b) AI professionals emphasize technical safeguards and self-regulation over rigid laws.
c) Youth want built-in privacy protections that are easy to understand and use.

These concerns emphasize the need for stronger alignment between AI privacy policies, system design, and user expectations. Addressing these issues requires a combination of privacy education, clear transparency measures, enforceable regulations, and privacy-enhancing technologies to ensure AI systems support both privacy protection and responsible innovation.

4.5 PEA-AI Model

The Privacy-Ethics Alignment in AI (PEA-AI) Model is a stakeholder-driven framework that integrates privacy concerns, ethical considerations, and AI governance through continuous engagement with key stakeholders. Developed using a Grounded Theory approach, the model is directly shaped by real-world experiences rather than theoretical assumptions. It provides a structured process for aligning AI development with privacy expectations, ensuring that AI systems remain transparent, user-centered, and adaptable over time.

As illustrated in Fig 6, the PEA-AI Model development follows a structured cycle to integrate privacy ethics into AI development. It begins with Stakeholder Perception, gathering insights from young digital citizens, parents/educators, and AI professionals. These perspectives are analyzed in the Data Integration phase, where quantitative and qualitative findings are combined to build a comprehensive understanding of privacy risks. Based on these insights, Framework Development creates a negotiation-based privacy model that incorporates stakeholder expectations. The next step, Policy Alignment, ensures AI governance structures match real-world expectations, making privacy policies both practical and enforceable. Once aligned, Ethical Implementation embeds

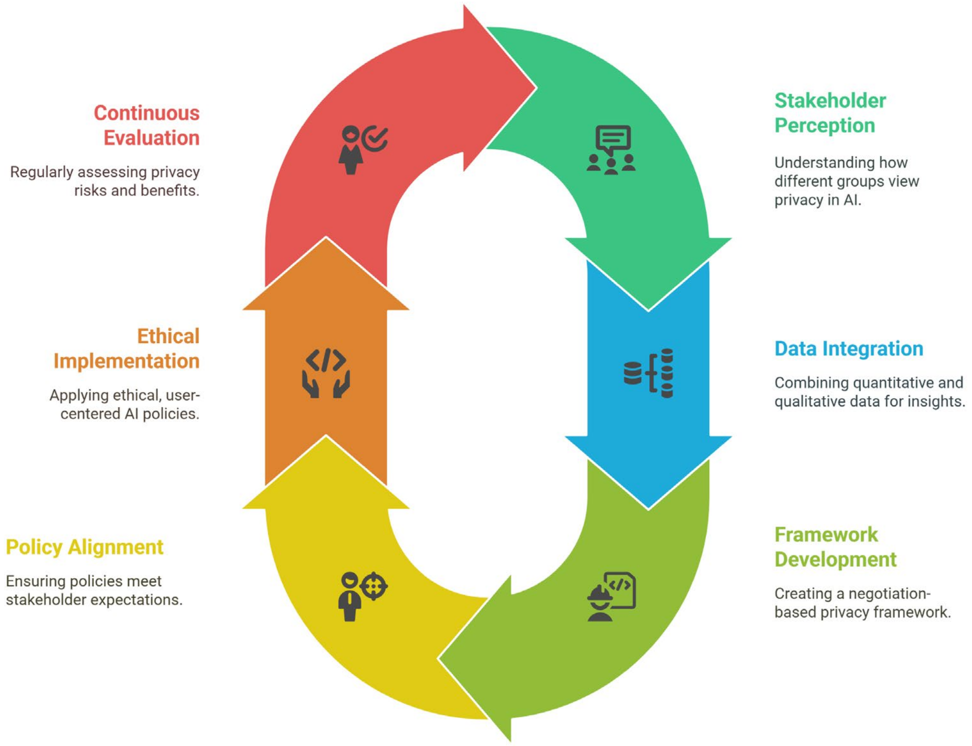
Continuous Evaluation
Regularly assessing privacy risks and benefits.
Stakeholder Perception
Understanding how different groups view privacy in AI.
Ethical Implementation
Applying ethical, user-centered AI policies.
Data Integration
Combining quantitative and qualitative data for insights.
Policy Alignment
Ensuring policies meet stakeholder expectations.
Framework Development
Creating a negotiation-based privacy framework.

Fig. 6. Grounded Theroy for PEA-AI Model Development

privacy and transparency directly into AI systems as core, built-in features rather than add-ons. Finally, since privacy risks evolve, the model emphasizes Continuous Evaluation, ensuring ongoing assessment and adaptation of AI privacy frameworks. This cyclical approach ensures that AI privacy is not static but instead a dynamic, ongoing process that evolves alongside technological advancements and societal expectations.

1) Positioning of the PEA-AI Model in AI Privacy Research

The PEA-AI Model builds upon foundational privacy theories, such as the Privacy Calculus Model (PCM) and Communication Privacy Management (CPM), but extends their applicability to AI governance and stakeholder negotiation.

- Privacy Calculus Model (PCM) emphasizes that individuals weigh risks and benefits when sharing personal data. The PEA-AI Model expands on this concept by incorporating stakeholder-driven negotiations into privacy governance, recognizing that privacy decisions are shaped not only by individual calculations but also by external factors such as policy regulations, digital literacy, and AI system design.
- Communication Privacy Management (CPM) focuses on how individuals manage privacy boundaries in communication. The PEA-AI Model broadens this scope by incorporating multi-stakeholder interactions, highlighting how youth, parents, educators, and AI professionals collaboratively influence AI privacy policies.

Rather than focusing solely on individual decision-making, the PEA-AI Model examines privacy as a collective, evolving process, shaped by negotiation between multiple stakeholders, regulatory frameworks, and technological advancements.

2) The PEA-AI Model as a Negotiation Framework

As illustrated in Fig. 7, the PEA-AI Model maps key privacy constructs—such as Data Control, Transparency, Trust, Parental Data Sharing, Perceived Risks and Benefits, and AI Privacy Awareness—to their impact on Ethical AI Development. It introduces a multi-stakeholder negotiation process, addressing four key tensions in AI privacy governance:

- Data Control vs. Trust – Balancing youth autonomy over data with AI developers' responsibility to mitigate risks.
- Transparency vs. Perception – Addressing the gap between AI disclosures and how users interpret transparency efforts.

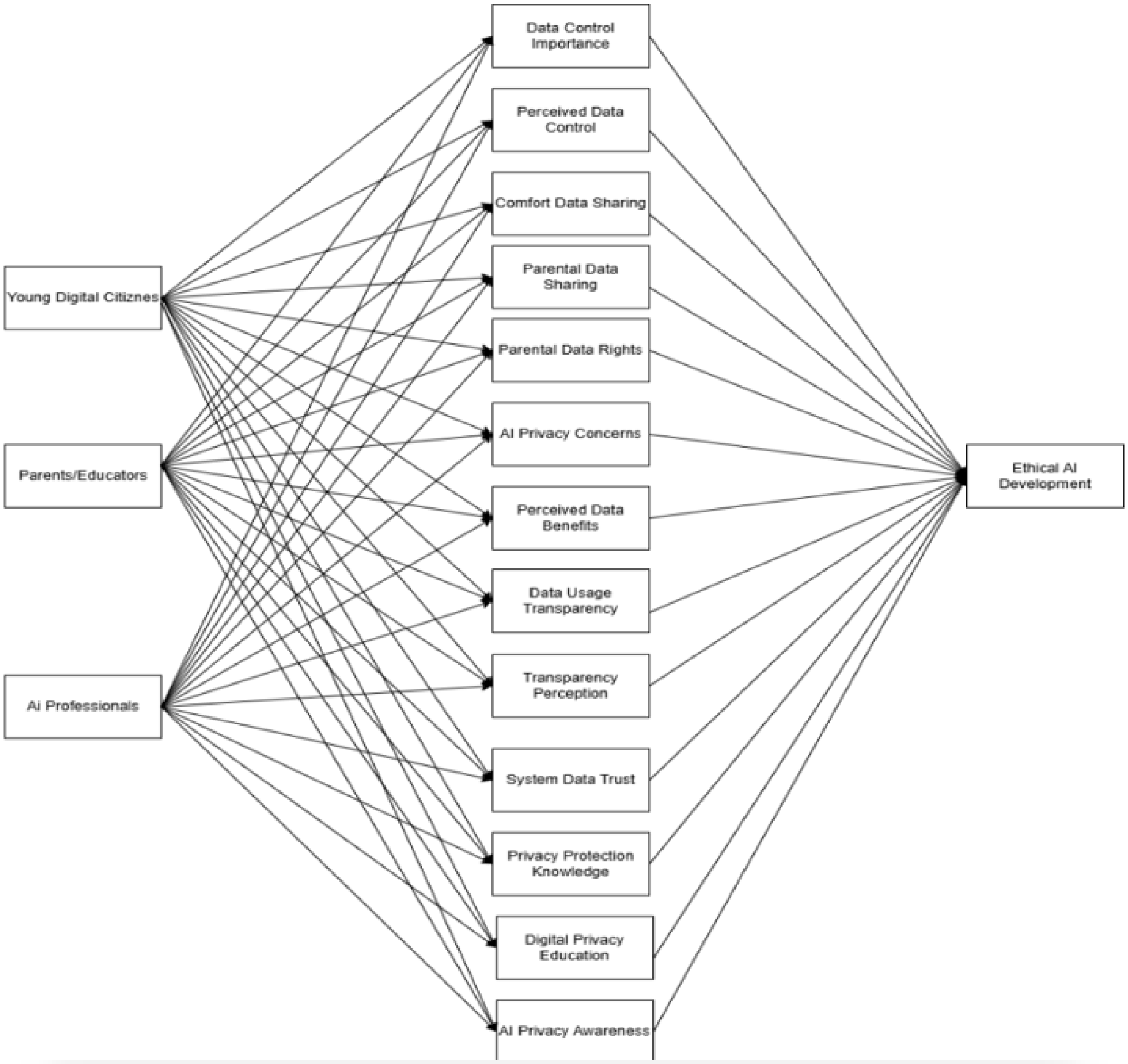

Fig. 7. PEA-AI Modle – Stakeholder Perspectives Leading to Ethical AI Development

- Parental Rights vs. Youth Autonomy – Negotiating consent mechanisms that respect youth decision-making while addressing parental concerns.
- Privacy Education vs. Awareness Deficit – Strengthening digital literacy to help users make informed AI privacy decisions.

Findings from the model highlight distinct privacy expectations among different groups:

- Young digital citizens value autonomy but often prioritize convenience over data control.
- Parents and educators emphasize security and regulatory protections but face challenges in AI literacy.
- AI professionals focus on system performance, compliance, and risk mitigation, while acknowledging the complexities of achieving full transparency.

By treating privacy as a negotiation rather than a fixed rule, the PEA-AI Model ensures that AI governance adapts to evolving stakeholder expectations rather than imposing a one-size-fits-all approach.

3) Applications of the PEA-AI Model in Research and AI Governance

The PEA-AI Model serves as a flexible and adaptable tool for researchers, policymakers, and AI developers. It can be utilized in several key areas:

- Empirical AI Privacy Research – Researchers can apply the model to study how privacy attitudes vary across different AI applications, such as personalized learning, facial recognition, and recommendation systems.
- AI Governance and Policy Development – Policymakers can use the model to create adaptive privacy regulations, ensuring that AI governance aligns with youth privacy needs, parental oversight, and industry standards.
- AI System Design and Development – AI developers can integrate the model into privacy-by-design frameworks, ensuring that AI systems provide clear, user-friendly privacy controls aligned with stakeholder expectations.
- Cross-Cultural AI Privacy Studies – The model can be applied to examine privacy perceptions across different cultural and legal environments, helping to develop globally adaptable AI policies.

By treating AI privacy as an evolving, stakeholder-driven negotiation, the PEA-AI Model provides a scalable and inclusive approach to AI governance. The model ensures that AI development remains responsive to real-world privacy concerns, promoting systems that are transparent, ethically aligned, and user-centered. Unlike static privacy models, the PEA-AI Model enables ongoing adaptation, ensuring that AI systems remain accountable and aligned with evolving societal expectations.

5. Guidelines Development and Policy Recommendations

This research resulted in the development of a set of draft guidelines to address the identified concerns, with an emphasis on practicality, inclusivity, and adaptability in various AI contexts. These guidelines incorporate best practices for parents, educators, AI developers, and youth to ensure responsible AI privacy management, and are discussed in detail in [26].

5.1 Guidelines Refinement Process

- Stakeholder Engagement: Feedback from interviews, focus groups, webinars, seminars, and conferences like IEEE CCWC and ICAIC guided iterative revisions to the guidelines.
- Policy Alignment: The team compared recommended practices with existing frameworks such as PIPEDA, GDPR, and emerging provincial legislation to ensure relevance.
- Expert Consultations: Discussions with AI ethicists, developers, and legal advisors refined the actionable steps for schools, technology companies, and parents.

5.2 Best Practices

These overarching principles apply to parents, educators, AI developers, and youth alike.

1) *Informed Consent and Age-Appropriate Notices*

    - Clear Opt-Ins: Provide straightforward, easy-to-understand consent forms explaining why data is collected and how it will be used.
    - Multi-Format Engagement: Use a mix of text, visuals, and short explainer videos to improve comprehension, especially for younger audiences.
    - Ongoing Awareness: Prompt youth to review their settings or data-sharing preferences periodically.

2) *Privacy by Design*

    - Data Minimization: Collect only essential data points needed for AI functionality.
    - Secure Storage and Transfer: Implement encryption for data at rest and in transit, ensuring limited access.
    - User-Friendly Tools: Offer accessible privacy dashboards where users can delete or download their data easily.
    - Anonymization: Where possible, replace identifiable data with anonymized or pseudonymized versions to enhance privacy while still allowing AI functionality.
    - Privacy Impact Assessments (PIAs): Conduct privacy impact assessments to evaluate how AI systems handle data, identify risks, and implement necessary safeguards.

- Default Privacy Protections: Ensure that AI applications, especially those used by youth, have privacy-enhancing settings enabled by default rather than requiring users to opt in manually.

3) Transparency and Explainability

- Plain-Language Policies: Use clear, jargon-free language to describe AI processes and data handling.
- Algorithmic Transparency: Offer general explanations of how AI makes decisions, especially for educational or recommendation systems.
- Stakeholder Feedback Loops: Invite regular input from students, parents, and educators regarding AI's perceived fairness and safety.

4) Monitoring and Accountability

- Internal Audits: Regularly audit AI systems for data leaks, biases, or security vulnerabilities.
- Reporting Mechanisms: Encourage users to report privacy concerns or AI errors swiftly (e.g., via dedicated forms or a helpdesk).
- Independent Oversight: Engage neutral experts, ethicists, or advisory groups to evaluate AI's impact on youth privacy and fairness.
- Ethical Data Handling Policies: Establish clear policies for responsible data use, ensuring that AI systems align with privacy regulations and ethical guidelines.

5) Multi-Stakeholder Collaboration for Safer AI

- Inclusive AI Policy Development: Policymakers, educators, AI developers, and youth representatives should collaborate to design AI applications with youth privacy in mind.
- Institutional Advocacy for AI Ethics: Schools and institutions can champion youth-centric AI policies that prioritize fairness, security, and informed consent.

5.3 Step-by-Step Guides

1) Educators and School Administrators

- Assess AI Tools: Review and vet AI-powered software for adherence to privacy laws and best practices.
- Obtain Appropriate Consents: If required, secure parental or guardian consent before introducing AI tools in the classroom.
- Integrate Privacy Lessons: Develop mini-lessons or modules teaching students about responsible data sharing and AI ethics.
- Monitor Usage and Feedback: Periodically check how students interact with AI software, gathering input on usability and privacy concerns.

2) Parents and Guardians

- Stay Informed: Familiarize yourself with the AI apps your children use, reviewing privacy policies and data-sharing terms.
- Set Boundaries: Guide children on safe data-sharing practices, encouraging them to question the necessity of certain permissions.
- Use Parental Controls: Enable built-in parental settings or external monitoring tools where applicable, balancing oversight with respect for autonomy.
- Ongoing Communication: Discuss with your child the reasons behind privacy settings, fostering a critical awareness of potential risks.

3) AI Developers and Researchers

- Incorporate Privacy by Default: Embed data minimization and secure architectures from the outset.
- Conduct Impact Assessments: Evaluate the ethical and privacy implications of AI on young users before deployment.
- Engage with Youth Feedback: Whenever possible, co-design features with the input of teenage end users to ensure real-world relevance.
- Comply with Standards and Regulations: Align development practices with OPC guidelines, PIPEDA, GDPR (if applicable), and local educational policies.

4) Young Digital Citizens

- Ask Questions: If unsure why an AI tool requests personal data, seek help from a teacher, parent, or trusted adult.
- Check Settings Regularly: Customize permissions (e.g., camera, microphone) and review your profile info to maintain control.
- Identify Suspicious Requests: Be cautious of apps asking for excessive personal details—report to a trusted adult when in doubt.
- Stay Curious and Critical: Learn basic concepts of how AI works, so you can better understand the implications of data sharing.

5.4 Proposed Policy Recommendations

- Mandatory Transparency Statements: AI platforms targeting minors should disclose data flow, storage durations, and processing methods in plain language.
- Consent Management: Implement tiered consent forms that acknowledge parental oversight but also empower youth autonomy where appropriate.
- Privacy Education Initiatives: Encourage integration of AI privacy topics into school curricula and promote awareness campaigns for parents and students.

6. Research Dissemination and Publications

This study employed a robust dissemination strategy, targeting academic, industry, and public channels to maximize the impact of its findings.

6.1 Conference Presentations

1) 2024 IEEE 15th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) – University of California, Berkeley (October 24–26, 2024):
    a. PI presented the paper “Navigating AI to Unpack Youth Privacy Concerns: An In-Depth Exploration and Systematic Review.” This was awarded both the Best Paper Award and the Best Presentation Award. The research provided a comprehensive analysis of youth privacy concerns in AI systems, contributing to ongoing discussions on ethical AI and privacy governance.
2) 2025 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) – University of Nevada, Las Vegas (January 6–8, 2025)
    a. PI presented two papers, including “Toward Ethical AI: A Qualitative Analysis of Stakeholder Perspectives,” which earned the PI a Best Presenter Award.
    b. The second paper, “Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis,” was also presented, contributing to discussions on youth privacy and AI ethics.
    c. PI chaired a session on Security, Trust, and Privacy, drawing attention to the unique vulnerabilities of youth in AI systems.
3) 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC) – University of Houston, Texas (February 5–7, 2025)
    a. PI presented a paper “Applying Communication Privacy Management Theory to Youth Privacy Management in AI Contexts”.

6.2 Additional Invited Speaker Engagement

The PI was invited as an “invited speaker” at the ACM Seventh International Conference on Blockchain Technology and Applications (ICBTA) in Xi’an, China (December 6–8, 2024). The presentation “Building Trust and Transparency in the Era of Decentralized AI Systems” discussed the project’s findings and how distributed ledger technologies could reinforce privacy controls, sparking discussions that influenced the project’s guidelines refinement.

6.3 Peer-Reviewed Publications

- Frontiers in Computer Science (“Under Review”): The first journal paper, “Young Digital Citizens and Privacy in AI Systems: A Systematic Review of Perceptions, Concerns, and Expectations,” [27] submitted here has experienced delays due to reviewers being reassigned. The research team is proactively monitoring progress but notes challenges in meeting initial publication timelines.

- IEEE Access Submission ("Under Review"): The consolidated manuscript, "Unpacking Youth Privacy Management in AI Systems: A Privacy Calculus Model Analysis," [3] was submitted here. It combines the quantitative SEM findings with in-depth qualitative insights, proposing actionable recommendations for privacy regulators, schools, and AI developers.
- 2024 IEEE 15th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON): The award-winning paper "Navigating AI to Unpack Youth Privacy Concerns: An In-Depth Exploration and Systematic Review" [1] is published in IEEE Xplore, enhancing discourse on youth privacy and ethical AI governance.
- 2025 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC): Two papers,
  - "Toward Ethical AI: A Qualitative Analysis of Stakeholder Perspectives," [28] and
  - "Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis" [29]

  were published at this peer-reviewed IEEE conference proceedings. The conference featured rigorous peer review, presentation, and discussion, contributing to the scientific community's understanding of ethical AI and youth privacy challenges. The full regular papers have been published in IEEE Xplore following this process.

- 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC): The paper "Applying Communication Privacy Management Theory to Youth Privacy Management in AI Contexts" [5] has been published in IEEE Xplore, following the IEEE peer-review process. To enhance accessibility, a preprint is also available on ResearchGate, ensuring broader dissemination beyond subscription-based platforms.

7. Public Engagement and Knowledge Mobilization

This project has prioritized public outreach, ensuring that findings resonate beyond academia and shape real-world practices.

7.1 Project Website and Social Media

- The project website *Privacy-Aware AI for Youth*[7] centralizes updates, publications, and educational resources.
- Medium Articles: The following articles have highlighted key milestones and core messages of the project, drawing public interest and engagement.
    - Empowering the Next Generation: Safeguarding Young Digital Citizens' Privacy in AI Systems[8],
    - Navigating AI and Privacy: Celebrating Excellence at IEEE IEMCON 2024, UC Berkeley[9],
    - Championing Privacy-Centric AI: Reflections from IEEE CCWC 2025 at UNLV[10],
    - Exploring AI and Privacy: Reflecting on IEEE ICAIC 2025 at the University of Houston[11], and
    - Bridging Ethics and Innovation: Insights from the Vancouver AI Meetup[12].

7.2 Media Coverage and Community Engagement

The research team has actively engaged with the media and the community to disseminate research findings and raise awareness on youth privacy in AI systems. The following initiatives contributed to outreach and knowledge mobilization.

- The Jas Johal Show (Global News)[13]: The Principal Investigator (PI) participated in an interview discussing youth perspectives on AI privacy, emphasizing concerns regarding data transparency, the need for stronger regulations, and the role of education in empowering young users to manage their digital privacy.
- VIU Fest Participation[14]: The research team presented preliminary findings through an interactive booth, fostering engagement with students, parents, and faculty. Attendees were

[7] https://csci-viu.github.io/privacy-aware-ai-for-youth/

[8] https://medium.com/@PrivaLab/empowering-the-next-generation-safeguarding-young-digital-citizens-privacy-in-ai-systems-ae29cb22f4f5

[9] https://medium.com/@PrivaLab/navigating-ai-and-privacy-celebrating-excellence-at-ieee-iemcon-2024-uc-berkeley-23dfdec3996d

[10] https://medium.com/@PrivaLab/championing-privacy-centric-ai-reflections-from-ieee-ccwc-2025-at-unlv-f617a869f40e

[11] https://medium.com/@PrivaLab/navigating-ai-and-privacy-reflecting-on-ieee-icaic-2025-at-the-university-of-houston-1f6a74deeaaa

[12] https://medium.com/@PrivaLab/bridging-ethics-and-innovation-insights-from-the-vancouver-ai-meetup-cbade5b4492f

[13] https://open.spotify.com/episode/1mnBgwld75OyvcUaa8dlKn?si=b4AdTApYTiqGAxJlf8Z-RA

[14] https://medium.com/@PrivaLab/connecting-with-the-community-at-viu-fest-a-step-forward-for-ai-privacy-be24879e5ac1

invited to share feedback, participate in surveys, and explore opportunities to contribute to the study.

- Media Coverage & Research Dissemination:
    - The Nanaimo News Bulletin published an article[15] in September 2024 titled "VIU Researcher Studying Youth Opinions on AI," featuring an interview with the PI. The article provided content for journalists to report on privacy issues affecting Canadians and highlighted the study's focus on AI privacy, youth concerns, and digital literacy. Through this coverage, the research helped raise public awareness on the implications of AI technologies for young users, emphasizing the need for stronger privacy protections and ethical AI governance.
    - Another interview with the Nanaimo News Bulletin is scheduled for the last week of March 2025 to discuss the final research findings on youth privacy in AI. Additionally, an article covering these findings is being developed in collaboration with The Conversation Canada[16] to facilitate wider public engagement and knowledge dissemination on the ethical and privacy implications of AI for young users.
- LinkedIn, X, and Facebook Posts: Regular updates on PI and research team members' personal social media channels, as well as Vancouver Island University's official media handles, provided quick insights into ongoing developments, new publications, and conference highlights. The VIU News article[17] on AI privacy concerns among young users has been widely shared across social platforms, contributing to broader engagement and discussion.

7.3 Webinar on Privacy Laws and AI (March 7, 2025)

The webinar "Privacy Laws and AI: Navigating Emerging Challenges[18]" was successfully organized as an online event via Microsoft Teams, engaging 40 registered participants, including students, faculty, and professionals.

The session fostered meaningful discussions on AI privacy, ethics, and policy developments. Dr. Ajay Shrestha presented key findings from the OPC-funded research, introducing the Privacy-Ethics Alignment in AI (PEA-AI) model, which highlights the ethical considerations and stakeholder expectations in AI development. Expert speakers from the Ministry of Citizens' Services—Colleen Rice (Executive Director, Strategic Policy, Privacy, and Legislation), Kirsten Nicholson (Director of Policy and Legislation), and Caitlin Buck (Director of Policy and Legislation)—provided in-depth insights into BC's privacy laws, their implications for AI governance, and children's privacy protections.

[15] https://www.nanaimobulletin.com/home/viu-researcher-studying-youth-opinions-on-ai-7521334
[16] https://theconversation.com/ca
[17] https://news.viu.ca/viu-computer-science-professor-investigating-ai-privacy-concerns-among-young-users
[18] https://events.viu.ca/privacy-laws-ai-navigating-emerging-challenges

The session was highly informative, enhancing participants' understanding of data protection, responsible AI governance, and evolving privacy regulations. Attendees were encouraged to explore additional resources through the project website. The report[19] and recorded session[20] are available for educational purposes to further support knowledge dissemination.

7.4 Seminar on AI Ethics and Privacy (March 13, 2025)

The *AI Ethics and Privacy Workshop: Safeguarding Tomorrow's Data Landscape*[21] was successfully organized at Vancouver Island University (VIU) in the Madrona Room (Bldg. 305, Rm. 332) within the university library. This interactive session engaged approximately 45 participants, including students, educators, researchers, and professionals, fostering discussions on AI ethics, privacy concerns, and responsible AI governance.

The event began with an icebreaker activity, encouraging participants to reflect on AI's presence in daily life, followed by an introduction to key ethical concepts such as bias, fairness, transparency, and accountability. A case study discussion on AI bias in hiring prompted students to critically analyze ethical dilemmas, debating the advantages and risks of AI-driven recruitment. An interactive exercise using the "Survival of the Best Fit[22]" simulation allowed participants to experience how biases are embedded in AI algorithms.

Live AI demonstrations, including ChatGPT[23] discussions and AI-generated image[24] analysis, further highlighted algorithmic biases and transparency challenges. The session concluded with a Q&A and reflection period, where students shared their perspectives on ethical AI. To support engagement and participation, catering was provided, including lunch, coffee, and dessert.

As part of the event's ethical considerations, consent was obtained from all participants for recording the session. A designated area was allocated for individuals who did not wish to be recorded, ensuring their privacy. This area was strictly excluded from all recordings throughout the event.

This workshop successfully combined research insights with hands-on activities, equipping students with a foundational understanding of AI privacy, ethics, and responsible digital practices. A handbook[25] detailing the research findings, developed after a third iteration of feedback, was distributed to participants, provided to the library and various schools in the region, and made available online for broader access. The complete seminar report[26] and recorded session[27] are available as educational resources to support knowledge dissemination.

[19] https://csci-viu.github.io/privacy-aware-ai-for-youth/webinar-report.html

[20] https://youtu.be/Jpa277UnkVc

[21] https://viu-ca.libcal.com/calendar/events/AIEthics

[22] https://www.survivalofthebestfit.com/

[23] https://chatgpt.com/

[24] https://www.craiyon.com/

[25] https://csci-viu.github.io/privacy-aware-ai-for-youth/assets/reports/Booklet.pdf

[26] https://csci-viu.github.io/privacy-aware-ai-for-youth/seminar-report.html

[27] https://youtu.be/6JfZoaeVwxY

8. Challenges and Mitigation Strategies

1) School District Approval Delays:
   a. Challenge: Slowed youth recruitment and data collection.
   b. Mitigation: Extended data collection window, engaged directly with approved districts (SD62, SD68, SD79) and leveraged university events like VIU Fest to recruit participants.
2) Journal Review Delays:
   a. Challenge: Timely publications have been hindered by reviewer unavailability at Frontiers in Computer Science and IEEE Access.
   b. Mitigation: The research team pursued conference presentations and publications to maintain momentum. The research team has been actively monitoring the review process and maintaining communication with the journals' editorial offices to expedite progress.
3) Regulatory and Ethical Complexity:
   a. Challenge: Rapidly evolving AI technologies and diverse stakeholder needs require ongoing ethical review and policy alignment.
   b. Mitigation: Regularly consulted with REB, adapted data practices, and remained flexible in refining guidelines.
4) Resource and Time Constraints
   a. Challenge: Balancing a comprehensive study with limited staff and budgets.
   b. Mitigation: Delegation of tasks to undergraduate research assistants and volunteers, combined with the PI's active involvement in all aspects of the project, ensured streamlined project management. The PI played a hands-on role in data collection, analysis, manuscript preparation, and coordination, effectively balancing resource limitations while maintaining research quality and progress.

9. Conclusion and Next Steps

This report underscores how the Privacy-Aware AI for Young Digital Citizens project fulfilled its primary objectives, from robust data collection to the formulation of evidence-based guidelines. The key achievements include:

- Completing surveys, conducting interviews, and facilitating focus groups, resulting in a diverse and comprehensive dataset, capturing the nuances of youth privacy perceptions alongside insights from educators, parents, and AI professionals, enriching both quantitative and qualitative analyses.
- Demonstrating the viability of a mixed-methods approach (SEM and qualitative analysis) in analyzing complex socio-technical issues, identifying core privacy concerns, and developing targeted guidelines for users' AI privacy.
- Sharing results at major IEEE conferences such as IEEE IEMCON 2024, IEEE CCWC 2025, and IEEE ICAIC 2025, through journal submissions, a dedicated webinar featuring expert discussions, an in-person seminar on AI ethics and privacy, and various public forums. These efforts broadened the project's impact, facilitated stakeholder engagement, and provided opportunities to receive constructive feedback from the research community.

9.1 Future Research Directions

- **Continued Stakeholder Engagement:** Further collaboration with school districts, parents, AI developers, and policymakers to refine guidelines as AI tools evolve.
- **Expanding the Focus:** Investigate privacy risks in AI-powered smart devices, including voice assistants, connected vehicles, and wearable technology, to understand how personal data is collected, processed, and shared. This includes technical analysis, stakeholder consultations, and the development of privacy toolkits to empower individuals with stronger digital privacy practices.
- **Policy Implementation and Real-World Testing:** Pilot the recommended guidelines within select educational and AI development environments, measuring their effectiveness, feasibility, user satisfaction, and long-term impact on privacy awareness.
- **Longitudinal Studies:** Examine how youth privacy attitudes evolve over time, particularly as AI systems become more pervasive in daily life, while assessing the sustained effectiveness of implemented guidelines in fostering informed privacy practices.

9.2 Recommendations for Future AI Privacy Initiatives

- Encourage collaboration among educational authorities, policymakers, technology sectors, and AI developers to update guidelines as regulations and technologies evolve, ensuring that AI practices remain aligned with youth privacy needs.

- Foster alliances among computer scientists, sociologists, legal scholars, ethicists, and educators to co-create robust, ethical AI solutions, standardize best practices, and establish certification programs focused on AI ethics and privacy.
- Support long-term research funding to monitor and adapt guidelines as AI technologies rapidly advance.

9.3 Acknowledgment

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

9.4 Closing Remarks

This project has contributed vital insights into the privacy landscape affecting young digital citizens, highlighting strategies to uphold trust and transparency in AI. By documenting challenges, achievements, and clear next steps, this report confirms the enduring relevance of youth-centric privacy research. Going forward, the Principal Investigator (PI) remains committed to refining and disseminating the guidelines, advancing collaborative discussions, and supporting the OPC's broader mission to safeguard personal information in Canada's evolving digital spaces.

> *For any queries or additional information regarding this report, kindly contact the Principal Investigator. The research team appreciates the continued support of the OPC, VIU, and all participating school districts, volunteers, and stakeholders who made this project possible.*

References

[1] A. K. Shrestha *et al.*, "Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review," in *2024 IEEE 15th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Berkeley, CA, USA: IEEE, 2024, "in press".

[2] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006, doi: 10.1287/ISRE.1060.0080.

[3] A. Shouli, A. Barthwal, M. Campbell, and A. K. Shrestha, "Unpacking youth privacy management in AI systems: A privacy calculus model analysis," *IEEE Access*, 2025, "in review".

[4] S. Petronio, "Communication privacy management theory: What do we know about family privacy regulation?," *J Fam Theory Rev*, vol. 2, no. 3, pp. 175–196, Sep. 2010, doi: 10.1111/J.1756-2589.2010.00052.X.

[5] M. Campbell, S. Joshi, A. Barthwal, A. Shouli, and A. K. Shrestha, "Applying communication privacy management theory to youth privacy management in AI contexts," in *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, Houston, Texas, USA: IEEE, Feb. 2025, pp. 1–10. doi: 10.1109/ICAIC63015.2025.10848639.

[6] A. Barthwal, M. Campbell, and A. Shrestha, "Privacy Ethics Alignment in AI (PEA-AI): A Stakeholder-Centric Based Framework for Ethcial AI".

[7] L. Anselm and A. J. Cerniglia, *Excerpts from : The Discovery of Grounded Theory : Strategies for Strauss*. 2008. Accessed: Feb. 10, 2025. [Online]. Available: https://www.routledge.com/Discovery-of-Grounded-Theory-Strategies-for-Qualitative-Research/Glaser-Strauss/p/book/9780202302607

[8] P. B. Brandtzaeg, A. Pultier, and G. M. Moen, "Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy," *Soc Sci Comput Rev*, vol. 37, no. 4, pp. 466–488, Aug. 2019, doi: 10.1177/0894439318777706.

[9] Bélanger and Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly*, vol. 35, no. 4, p. 1017, 2011, doi: 10.2307/41409971.

[10] H. Xu, T. Dinev, H. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view," *ICIS 2008 Proceedings*, Jan. 2008, Accessed: Nov. 14, 2024. [Online]. Available: https://aisel.aisnet.org/icis2008/6

[11] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *https://doi.org/10.1287/isre.1040.0032*, vol. 15, no. 4, pp. 336–355, Dec. 2004, doi: 10.1287/ISRE.1040.0032.

[12] S. Livingstone and E. J. Helsper, "Parental mediation of children's internet use," *J Broadcast Electron Media*, vol. 52, no. 4, pp. 581–599, Oct. 2008, doi: 10.1080/08838150802437396.

[13] C. E. Koh, V. R. Prybutok, S. D. Ryan, and Y. "Andy" Wu, "A model for mandatory use of software technologies: An integrative approach by applying multiple levels of abstraction of informing science," *Informing Science: The International Journal of an Emerging Transdiscipline*, vol. 13, pp. 177–203, 2010, doi: 10.28945/1326.

[14] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Commun ACM*, vol. 42, no. 2, pp. 60–67, Feb. 1999, doi: 10.1145/293411.293475.

[15] A. K. Schnackenberg and E. C. Tomlinson, "Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships," *J Manage*, vol. 42, no. 7, pp. 1784–1810, Nov. 2016, doi: 10.1177/0149206314525202.

[16] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal*, vol. 25, no. 6, pp. 607–635, Nov. 2015, doi: 10.1111/isj.12062.

[17] G. R. Milne and M. J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *Journal of Interactive Marketing*, vol. 18, no. 3, pp. 15–29, Jan. 2004, doi: 10.1002/DIR.20009.

[18] P. A. Pavlou, "State of the information privacy literature: Where are we now and where should we go?," *MIS Q*, vol. 35, no. 4, pp. 977–988, 2011, doi: 10.2307/41409969.

[19] PuhakainenPetri and SiponenMikko, "Improving employees' compliance through information systems security training," *MIS Quarterly*, Dec. 2010, doi: 10.5555/2017496.2017502.

[20] T. Buchanan, C. Paine, A. N. Joinson, and U. D. Reips, "Development of measures of online privacy concern and protection for use on the Internet," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 157–165, Jan. 2007, doi: 10.1002/ASI.20459.

[21] A. K. Shrestha and J. Vassileva, "User acceptance of usable blockchain-based research data sharing system: An extended TAM-based study," *Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2019*, pp. 203–208, Dec. 2019, doi: 10.1109/TPS-ISA48467.2019.00033.

[22] W. W. Chin, B. L. Marcelin, and P. R. Newsted, "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study," *https://doi.org/10.1287/isre.14.2.189.16018*, vol. 14, no. 2, Jun. 2003, doi: 10.1287/ISRE.14.2.189.16018.

[23] A. K. Shrestha, J. Vassileva, S. Joshi, and J. Just, “Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system,” *PeerJ Comput Sci*, vol. 7, pp. 1–38, May 2021, doi: 10.7717/PEERJ-CS.502/SUPP-7.

[24] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*, Second. Thousand Oaks, California, United States, 2017.

[25] P. R. Warshaw and F. D. Davis, “Disentangling behavioral intention and behavioral expectation,” *J Exp Soc Psychol*, vol. 21, no. 3, pp. 213–228, May 1985, doi: 10.1016/0022-1031(85)90017-4.

[26] A. Shouli, A. Barthwal, M. Campbell, and A. K. Shrestha, “Ethical AI for Young Digital Citizens : A Call to Action on Privacy Governance”.

[27] A. K. Shrestha, A. Barthwal, M. Campbell, A. Shouli, and S. Syed, “Young digital citizens and privacy in AI systems: A systematic review of perceptions, concerns, and expectations,” *Front Comput Sci*, 2025, “in review”.

[28] A. K. Shrestha and S. Joshi, “Toward ethical AI: A qalitative analysis of stakeholder perspectives,” in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, Nevada, USA: IEEE, Jan. 2025, pp. 00022–00029. doi: 10.1109/CCWC62904.2025.10903879.

[29] M. Campbell, A. Barthwal, A. Shouli, S. Joshi, and A. K. Shrestha, “Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis,” in *presented at 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, Nevada, USA: IEEE, 2025.