IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 March 2025, accepted 24 April 2025, date of publication 3 July 2025, date of current version 10 July 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3585635

RESEARCH ARTICLE

Unpacking Youth Privacy Management in AI Systems: A Privacy Calculus Model Analysis

AUSTIN SHOULI, ANKUR BARTHWAL, MOLLY CAMPBELL, AND AJAY KUMAR SHRESTHA, (Member, IEEE)
Department of Computer Science, Vancouver Island University, Nanaimo, BC V9R 5S5, Canada

Corresponding author: Ajay Kumar Shrestha (ajay.shrestha@viu.ca)

This work was supported by the Office of the Privacy Commissioner of Canada's (OPC) Contribution Programs.
This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Vancouver Island University Research Ethics Board (VIU-REB) under Approval No. 103116.

ABSTRACT The increasing use of Artificial Intelligence (AI) in daily life has introduced substantial issues in protecting user privacy, particularly for young digital citizens. This study examines the complex dynamics of privacy management in AI systems utilizing the Privacy Calculus Model (PCM), with 482 participants: 176 young digital citizens (ages 16–19), 146 parents and educators, and 160 AI specialists. The research used a mixed methods approach to analyze key characteristics, including data ownership, user control, parental data sharing attitude, transparency, trust, perceived risks, benefits, and education. The results underscore the necessity of promoting digital literacy, establishing trust through transparent practices, and implementing collaborative approaches for privacy governance. The study emphasizes the significance of customized educational activities and regulatory frameworks that enable users to manage the trade-offs between the advantages and risks of data sharing by including varied views. This research enhances ethical AI development and advocates equal privacy safeguards for children and young adults.

INDEX TERMS Data ownership, education, ethical artificial intelligence, parental data sharing, privacy calculus theory, transparency, trust, user control, youth.

I. INTRODUCTION

Artificial Intelligence (AI) has blended into several aspects of contemporary life, providing transformational capacities in fields such as education, healthcare, and social media. Among its users, young digital citizens, also referred to as digital natives, have a distinctive role in the technological environment owing to their early and frequent engagement with AI-driven systems [1]. The concept of digital citizenship extends beyond basic internet access, encompassing responsible and ethical engagement within digital environments. This includes awareness of data privacy, online safety, and the ethical use of AI technologies. As AI becomes more embedded in everyday interactions, digital citizenship is evolving to emphasize not only the skills required to navigate digital spaces but also the associated rights and responsibilities of users, particularly youth [2], [3].

Although these technologies utilize personal data to improve user experiences, their extensive data-gathering methods have generated considerable privacy issues, especially for younger users who may be unaware or unprepared to protect their personal information [4]. Unlike older generations, who typically adopted digital technologies later in life, young digital citizens often do not have a concrete understanding of data ownership, long-term digital footprints, or the risks associated with uninformed data sharing. This gap in awareness is further exacerbated by algorithmic personalization, which subtly shapes user behavior and information exposure, sometimes at the expense of privacy and autonomy [5].

While AI has significant advantages such as customization and efficiency, it also presents concerns associated with data exploitation, loss of control, and ethical challenges [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Claudia Raibulet.

The standardized dissemination of personal information on social media, along with a deficient comprehension of data aggregation methods, renders young users more susceptible to privacy breaches and exploitation. The growing pervasiveness of AI in social media platforms, educational tools, and digital assistants amplifies these risks, raising ethical questions about informed consent and data transparency [7]. These problems highlight the necessity for a comprehensive analysis of how young digital citizens manage the trade-offs between the risks and benefits linked to AI technology [4].

Our research employs the Privacy Calculus Model (PCM) to examine these dynamics, providing a structured framework for understanding young digital users' decision-making regarding data sharing. PCM asserts that users evaluate the perceived advantages of data sharing, such as ease and personalization, against the corresponding dangers, including possible privacy infringement and data exploitation [4]. This model is augmented by five interconnected constructs in our case: Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA) [3]. These constructs provide a thorough examination of how individual attitudes, parental influences, and technology factors impact youth privacy management practices.

Our study used a mixed-methods approach, conducting both quantitative analysis through structured surveys and qualitative exploration via open-ended responses, interviews, and focus groups. The participant pool comprises AI developers and researchers, parents, educators, and young digital citizens aged 16 to 19. The research employs Partial Least Squares Structural Equation Modelling (PLS-SEM) to identify key factors influencing young digital citizens' privacy decisions, emphasizing the significance of transparency, trust, and digital literacy in mitigating privacy risks [4].

The results emphasize the need to empower young users through targeted educational programs, build trust in AI systems with transparent data practices, and support informed decision-making. These insights contribute to the broader conversation on developing user-focused and ethically responsible AI technology while shaping regulations to address the unique privacy needs of young digital citizens.

The rest of the paper is organized as follows: Section II provides background and reviews relevant literature. Section III outlines the methodology. Section IV presents the findings. Section V discusses implications and future research directions. Section VI concludes the paper.

II. BACKGROUND AND RELATED WORKS

A. PRIVACY CALCULUS MODEL FOR YOUTH PRIVACY IN AI

The Privacy Calculus Model (PCM) offers a thorough framework for understanding how individuals assess perceived risks and rewards when deciding to share personal information. In contrast to conventional models, PCM emphasizes the cognitive and environmental elements that affect privacy decisions. For young digital citizens, these choices are influenced by developmental characteristics, digital literacy, and regular engagement with AI technology. Young individuals frequently emphasize immediate advantages, such as tailored content and ease, while undervaluing hazards such as data exploitation or breaches [8], [9].

PCM fundamentally asserts that consumers evaluate possible adverse consequences, such as loss of control, illegal access, or exploitation, against beneficial results like tailored services, enhanced user experiences, and increased convenience [2]. However, young users often prioritize short-term benefits over long-term privacy risks due to limited awareness of AI's data collection and predictive analytics. This behavior is particularly evident in contexts such as social media, gaming, and personalized educational platforms [10]. According to PCM, privacy decisions entail a reasonable trade-off in which users evaluate the immediate benefits of AI applications against the long-term consequences for data protection. Studies indicate that many adolescents engage with AI systems without fully understanding how their data is processed, stored, or utilized for predictive analytics and behavioral tracking [2].

The context of data sharing is crucial within PCM; for example, young individuals are often more inclined to provide information in trusted settings, such as educational or social media platforms, rather than in more sensitive areas like healthcare or finance. Furthermore, PCM underscores that privacy decisions are not fixed but may develop over time as consumers acquire additional information or as the perceived risks and advantages fluctuate. Research suggests that as young individuals become exposed to privacy breaches, parental guidance, or digital literacy programs, they adjust their privacy behaviors accordingly [7]. This temporal unpredictability is particularly evident in young users, whose cognitive and emotional frameworks are still maturing. Trust is a crucial element since confidence in the data-collecting institution profoundly influences privacy choices. Transparent data methods and ethical information management foster trust, promoting increased willingness among the users to share data.

Despite the extensive application of PCM to general privacy behaviors, its significance in teenage privacy management within AI contexts remains little examined. This research expands upon PCM by incorporating components such as Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA). This research enhances the theoretical application of PCM by tailoring it to the unique privacy issues encountered by adolescents in AI systems, offering practical guidance for the development of ethical, youth-focused AI technology [11].

B. PRIVACY CHALLENGES FOR YOUNG DIGITAL CITIZENS

Young digital citizens, known as digital natives [3], interact heavily with AI systems via social media, educational tools, and gaming applications. These interactions subject users to considerable privacy threats, including illegal data access, targeted advertising, and profiling [12], [13]. Despite heightened awareness of these concerns, numerous young users lack the knowledge and abilities to manage complex privacy settings or fully understand the consequences of their data-sharing decisions [14]. A significant difficulty exists in the disparity between the extensive digital participation of young users and their inadequate capacity to manage privacy proficiently. Prominent data breaches and unethical data practices have heightened concerns, while the opacity of AI systems and convoluted data regulations sometimes render young users feeling powerless [8]. Parental influence introduces an additional degree of complexity to this matter. While parents often aim to assist their children in managing privacy, excessive interference can unintentionally undermine adolescents' autonomy, resulting in conflicts between independence and control [13]. Furthermore, deficiencies in digital literacy instruction impede young users from acquiring proficient privacy management abilities. Research indicates that digital literacy profoundly influences privacy behaviors; nevertheless, existing educational programs frequently neglect the distinct issues presented by AI technology [14], [15]. To address these deficiencies, it is essential to prioritize transparency and trust in AI systems while providing young digital citizens with the necessary tools and information to understand and exercise their privacy rights.

C. BRIDGING GAPS IN PRIVACY RESEARCH AND PRACTICE

Despite extensive research on privacy concerns and behaviors, the majority concentrates on adult populations or broad user groups, resulting in a deficiency in understanding the experiences of young digital citizens in AI situations. Current research underscores the significance of transparency, dependability, and ethical issues in cultivating confidence in AI systems [16], [17]. The Privacy Calculus Model (PCM) has been extensively utilized to investigate privacy decision-making in domains such as e-commerce, social media, healthcare and other sectors [18], [19], yet it has not been employed to address the particular challenges encountered by youth in navigating privacy within AI-driven contexts. This study fills these gaps by utilizing PCM on empirical data gathered from young digital citizens, parents, educators, and AI professionals, marking the first investigation of youth privacy management in AI contexts using this framework. It underscores the interaction among perceived risks, advantages, and trust, elucidating how young users manage privacy within AI contexts. Moreover, it underscores the necessity of incorporating stakeholder perspectives into AI design and governance to develop ethical frameworks that safeguard young users while monitoring the evolution of privacy views as AI technologies become increasingly integrated into everyday life [20].

D. ADAPTING THE PRIVACY CALCULUS MODEL TO AI-DRIVEN YOUTH PRIVACY CONCERNS

In fields like social media, healthcare, and e-commerce, where consumers logically weigh the advantages and disadvantages of disclosing personal information, the Privacy Calculus Model (PCM) has historically been used. AI-driven ecosystems, however, present a new set of privacy issues, especially for young digital citizens who might not have the knowledge or mental development to understand intricate data-processing systems. AI systems, in contrast to traditional digital platforms, process data independently, infer behavioral patterns, and learn from users continuously, making privacy trade-offs far less obvious. The static risk-benefit analysis typically associated with PCM is challenged by the dynamic nature of AI, which calls for its expansion to take into consideration dynamic, automated, and occasionally opaque data-collecting processes [7].

The ongoing and inferred nature of data processing is a significant difference between AI and traditional digital environments. Even while young users might not provide much explicit data, AI systems employ machine learning algorithms to derive a wealth of behavioral insights. This implies that personal profiles are continuously updated and improved, frequently without the subject's knowledge, even in the absence of express agreement. According to studies, even if they are tech-savvy, teenagers frequently find it difficult to understand the long-term effects of algorithmic decision-making, predictive analytics, and AI-driven [10]. AI-driven platforms function constantly, requiring young users to navigate an environment where data-sharing ramifications are not instantaneous nor easily understood, in contrast to classic PCM applications, where users make explicit trade-offs in limited instances.

PCM applications are made more difficult by the critical role parental mediation plays in influencing young people's privacy behaviors in AI environments. By imposing rules, offering advice, or unintentionally disclosing their children's information through actions like "sharenting"-the parental sharing of children's personal information on social media and other AI-enabled platforms-parents can affect how their kids use AI-powered platforms. According to research, parents who actively participate in their kids' digital lives can reduce privacy threats by raising awareness and promoting appropriate data-sharing practices. However, a lot of parents themselves don't fully get how AI handles data, which results in a lack of consistency in their privacy practices [10]. The evolving role of parental mediation in AI-driven privacy decision-making highlights the need for PCM to integrate external influences beyond individual user agency, as privacy decisions are often co-regulated rather than independently made.

Decisions about privacy must be made with transparency and trust, but AI ecosystems are frequently "black-box" systems that make it difficult for users, especially children, to understand how their data is handled and used. AI-driven platforms depend on intricate, automated decision-making processes that lack transparency, in contrast to conventional data-sharing agreements where risks and benefits are clearly stated. According to studies, consumers gain more trust and make better privacy decisions when AI platforms adopt explainable AI (XAI) [21] and transparent data regulations. On the other hand, opaque AI models increase privacy worries and decrease information-sharing willingness, especially among young users who rely on perceived trustworthiness to guide their privacy choices [2]. Therefore, the importance of algorithmic openness and trust-building methods in influencing young people's privacy views must be emphasized when adapting PCM to AI-driven scenarios. Furthermore, because it affects how well young users comprehend and react to AI-driven data gathering, digital literacy is a critical component in AI-specific privacy decision-making. AI environments add complexity that necessitates specific digital literacy training, in contrast to typical PCM applications that presume a fundamental understanding of privacy trade-offs. Young people frequently use AI-powered platforms without understanding how their data is processed, which leads them to underestimate the risks of data permanence and behavioral profiling. According to research, AI-specific literacy initiatives that emphasize data inference, algorithmic bias, and automated decision-making can provide young users with the information they need to make wise privacy decisions [5].

The use of PCM in AI-driven youth privacy management is made more difficult by ethical and legal issues. The present policies were mainly created for static digital environments with clearly defined user consent and explicit data collection. However, because AI-driven platforms rely on algorithmic decision-making, predictive modelling, and inferred data collection, they present privacy issues that are not adequately addressed by current legal frameworks. Research highlights the necessity of AI-specific privacy safeguards to control behavioral inference, improve algorithmic profiling's openness, and give minors a way to challenge or update AI-driven data representations [22]. Young users are still in danger from AI-driven privacy threats that go beyond conventional ideas of consent and control in the absence of strong legislative protections. The continuous discussion on managing youth privacy in automated digital environments is aided by the expansion of PCM to take into consideration the dynamic character of AI-driven ecosystems. AI environments necessitate an adaptive framework that takes into account ongoing data processing, parental mediation, algorithmic transparency, gaps in digital literacy, and changing legislative requirements, in contrast to traditional privacy models that presume logical and static trade-offs. To create ethical AI systems that emphasize openness, user control, and educated decision-making for young digital citizens, policymakers, educators, and AI developers must work together to ensure that young people can interact with AI technology without jeopardizing their privacy and digital autonomy, PCM's development in this context emphasizes the need for an interdisciplinary approach to AI privacy control.

III. METHODOLOGY

A. RESEARCH GOALS AND QUESTIONS

The principal objective of this study was to apply the Privacy Calculus Model (PCM) as a conceptual lens to investigate how youth, parents and/or educators, and AI professionals view privacy risks and benefits within AI-driven environments. Specifically, we examined the interplay among 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). By exploring these constructs, we aim to uncover how youth and stakeholders navigate the trade-offs between privacy risks and the perceived benefits of AI technologies. Guided by this framework, we addressed the following Research Questions (RQs), each of which draws on the PCM constructs:

1) **RQ1**: How do perceived risks associated with sharing personal data with AI technologies influence youths' and stakeholders' perceptions of data ownership and control in youth data-disclosure decisions?

2) **RQ2**: What perceived benefits do youth and stakeholders attribute to AI technologies, and how do these benefits shape youths' willingness to share personal information and parents' willingness to share their children's data?

3) **RQ3**: How do transparency and trust in AI systems affect youths' decisions to disclose personal data?

4) **RQ4**: How do youth and parents manage boundaries (through rules, behaviors, and strategies) when interacting with AI technologies?

5) **RQ5**: How do education and awareness about AI, and broader ethical considerations, as perceived by youth and stakeholders, impact youth's sense of control and autonomy over their personal information?

Fig. 1 provides a visual representation of how these research questions are mapped to the five constructs to collect insights from stakeholders. These variables, informed by the research questions, converge to inform actionable insights for Ethical AI Development. The definitions of these constructs are provided in Table 1, which details their scope and focus within the study.

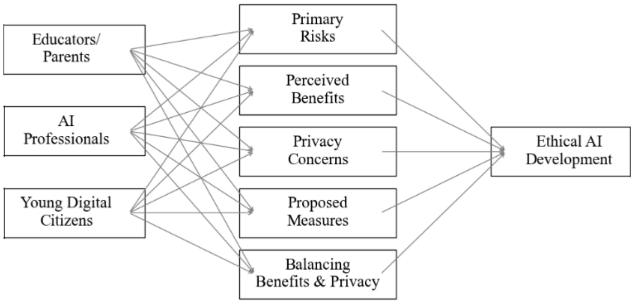


FIGURE 1. Stakeholder perspectives leading to ethical AI development.

TABLE 1. Constructs and definitions.

Construct	Definition
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.
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.
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.
Transparency and Trust (TT)	It is the degree to which transparency in data usage influences trust in AI systems.
Education and Awareness (EA)	It is the degree to which stakeholders are informed about privacy and ethical issues associated with AI.

B. RESEARCH MODEL AND HYPOTHESIS

Drawing upon insights from the literature [4], [19], [23], [24], particularly those emphasizing cost-benefit evaluations in AI adoption, we formulated fourteen hypotheses aligned with the above research questions. Each hypothesis was examined across four distinct groups—young digital citizens, parents and educators, AI professionals, and combined demographics—to explore how PCM's risk-benefit framework operates in varying contexts. Factors such as parental input, perceived control, and digital literacy were integrated to capture the full scope of privacy-related decision-making across these populations.

Below, the hypotheses are first presented in numerical order for consistency and ease of reference in the manuscript:

1) **H1**: DOC has a significant influence on PDS [25]
2) **H2**: PRB mediates the relationship between DOC and PDS [23]
3) **H3**: TT has a significant effect on PDS [26]
4) **H4**: PRB has a direct effect on PDS [27]
5) **H5**: DOC has a direct effect on PRB [28]
6) **H6**: EA has a direct effect on PRB [29]
7) **H7**: PRB mediates the relationship between TT and PDS [30]
8) **H8**: DOC has a direct effect on TT [31]
9) **H9**: TT has a direct effect on PRB [32]
10) **H10**: TT mediates the relationship between DOC and PDS [33]
11) **H11**: EA has a significant influence on PDS [34]
12) **H12**: EA has a total effect on TT [13], [35]
13) **H13**: EA has a direct effect on DOC [36], [37]
14) **H14**: PRB mediates the relationship between EA and PDS [33]

To systematically examine these relationships, the hypotheses are grouped below according to the research questions they address:

1) **RQ1**: H1, H2
2) **RQ2**: H4, H7
3) **RQ3**: H3, H8, H10
4) **RQ4**: H5, H9
5) **RQ5**: H6, H11, H12, H13, H14

C. RESEARCH DESIGN

The present 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 from three key demographic groups: Young Digital Citizens (aged 16-19), Parents and Teachers, and AI Researchers and Developers. These groups were purposefully selected to provide triangulation of perspectives, capturing the views of those who develop AI technologies, those who guide youth (parents and educators), and youth themselves.

Survey data was collected through convenience sampling, using a combination of recruitment methods, including flyers, personal networks, emails, and social networking platforms such as LinkedIn and Reddit. To reach our targeted youth demographic, we collaborated with several Vancouver Island school districts for their assistance in distributing our survey to their high school students. Youth participants were further recruited from Vancouver Island University (VIU) and personal networks. Educators were recruited from VIU, personal networks, and online platforms, while AI professionals were primarily recruited through personal networks and social networking sites.

Participation in the study was entirely voluntary, and participants did not receive any form of compensation. The participants had to read and accept a consent form before starting the questionnaire, indicating their understanding of the study's conditions. We conducted online surveys through Microsoft Forms to ensure accessibility and ease of participation.

Youth participants (aged 16–19) responded to the youth survey questions based on their own experiences and perceptions. Educators, parents, and AI professionals participated in separate surveys tailored to their roles and were not expected to answer on behalf of youth, but rather to provide their own perspectives on youth privacy and AI.

While this approach enabled efficient data collection, it introduces self-selection bias, as participation was voluntary, and individuals who chose to take part may possess distinct privacy orientations or heightened interest in the topic. This bias is particularly relevant in privacy research, where participants' motivations and sensitivities can shape their responses. Moreover, because youth and educator participants were primarily drawn from specific schools and universities in Canada, the sample may not reflect the full diversity of experiences across other regions. These limitations constrain the generalizability of our findings, but nonetheless offer valuable insights into the perspectives of these particular groups.

In addition to the survey questionnaires, we conducted interviews and focus groups with AI professionals, parents, and educators to gain deeper insights into their perspectives. 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, we conducted 12 interviews and 2 focus groups: one with 4 AI professionals and another with 5 parents and/or educators. Before the sessions, 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 questions for interviews and focus groups were tailored to each participant type to reflect their unique role and perspectives.

The survey instruments were adapted from constructs validated in prior studies [4], [18], [24], [36], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47]. 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) within these constructs are outlined in Table 2. Full survey prompts, interview and focus group scripts, as well as all consent forms, are provided in the Supplementary Material to ensure transparency and reproducibility.

TABLE 2. Constructs and items.

Construct	Items
Data Ownership and Control (DOC)	doc1: Importance of users having control over their personal data. doc2: Frequency of considering user data control in work. doc3: Feasibility/comfortability of implementing data control mechanisms.
Parental Data Sharing (PDS)	pds1: Handling data shared by parents on behalf of children. pds2: Importance of obtaining consent from young users.
Perceived Risks and Benefits (PRB)	prb1: Concern about ethical/privacy implications prb2: Significance of benefits in justifying data use. 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)	tt1: Importance of transparency about data usage. tt2: Perception of transparency in current AI systems. tt3: Belief that increasing transparency improves user trust.
Education and Awareness (EA)	ea1: Knowledge about privacy issues related to AI systems. ea2: Belief that users receive adequate training on privacy. ea3: Importance of being educated on privacy and ethical issues/ Adequacy of privacy information.

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 align 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).

D. PARTICIPANT DEMOGRAPHICS

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 parents and/or educators, 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 3 highlights the characteristics of the demographics of the participants.

IV. RESULTS

This study builds upon our previous research [48], [49], by expanding the sample to include more youth participants, allowing for a more robust and comprehensive analysis of their unique perspectives on privacy in AI systems. By incorporating insights from youth, parents, educators, and AI professionals, we aim to explore the privacy concerns and awareness levels of all three groups in greater depth, emphasizing their unique challenges and opinions in relation to AI and its implications for youth privacy, use, and protection.

Unlike our previous studies, which focused on consolidated datasets, this is the first study to analyze hypotheses across all three demographic groups: young digital citizens, parents and educators, and AI professionals. While this study compares the perspectives of these groups quantitatively and qualitatively, a formal analysis, such as multi-group analysis, was not conducted due to the scope of the paper. However, this approach provides a foundation for future research to explore group-specific differences in greater detail.

For data processing, Microsoft Excel was employed to manage the collected data through descriptive statistics. The analysis was conducted in all three demographic groups, as well as a consolidated dataset, to enable both group-specific and cross-group comparisons. We used a

TABLE 3. 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

partial least squares structural equation modeling (PLS-SEM) approach via smartPLS software [50]. PLS-SEM is a frequently utilized method to estimate path coefficients in structural models and is widely acknowledged in many studies [51], [52]. As suggested by [53], SEM involves testing measurement models (including exploratory factor analysis, internal consistency, convergent validity, and Dillon-Goldstein's rho) as well as the structural model through regression analysis. The path-weighting structural model scheme in smartPLS was employed to yield the highest R^2 values for dependent latent variables.

We additionally utilized a nonparametric bootstrapping procedure in our statistical analysis. Bootstrapping is a resampling technique that generates an empirical sampling distribution by repeatedly drawing samples with replacement from the original dataset. For our analysis, we produced 5,000 subsamples and conducted a two-tailed test at a significance level of 0.1.

In addition to the quantitative analysis, we conducted a thematic analysis of open-ended questions, interviews, and focus group discussions to identify common themes expressed by participants. This qualitative approach complements the quantitative findings by providing deeper insight into the stakeholders' perspectives and experiences, particularly in areas where quantitative data may not fully capture the nuances of privacy concerns.

A. DESCRIPTIVE STATISTICS

The quantitative survey revealed distinct patterns across 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) as shown in Fig. 2. AI developers and researchers rated DOC highest (3.95), followed by educators and parents (3.75) and young digital citizens (3.42). PDS scores were low across all groups, with AI professionals scoring 2,36, educators/parents scoring 2.94, and youth scoring 2,52.

PRB showed the most variation, with young digital citizens rating it highest at 3.98, educators and parents followed closely at 3.88, and AI developers and researchers significantly lower at 1.58. For TT, AI professionals scored 3.49, educators/parents scored 3.46, and youth scored 3.22. Similarly, for EA, AI developers and researchers scored highest at 4.16, followed by educators and parents at 3.43, and youth at 3.22.

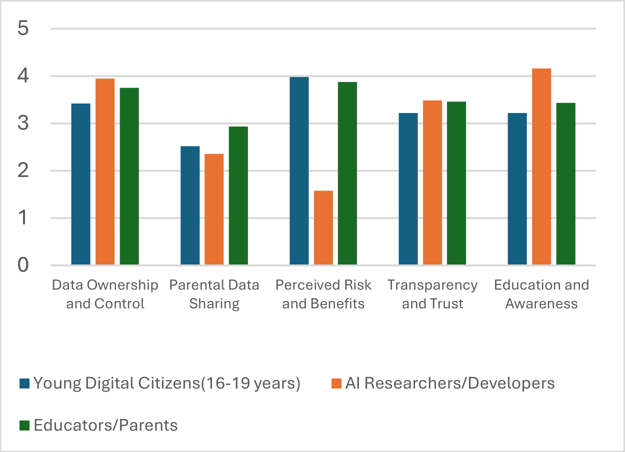


FIGURE 2. Means across constructs and demographics.

These results highlight differences in how the three groups perceive and prioritize privacy-related constructs, providing a foundation for further analysis and discussion.

B. MEASUREMENT MODELS

We evaluated the measurement model using exploratory factor analysis to assess the internal consistency, reliability, and validity of the constructs.

1) EXPLORATORY FACTOR ANALYSIS

For exploratory factor analysis, we first checked the factor loading of individual items shown in Table 4, to see whether each variable loaded highly on its own construct over the other respective constructs. Factor loadings exceeding 0.60 can be considered significant [54]. In our analysis, factor loadings varied across the four groups (AI professionals, educators/parents, young digital citizens, and combined demographics), suggesting that the constructs may operate differently for each group.

Item doc1 in the Data Ownership and Control (DOC) construct exhibited a strong loading for AI professionals (0.791) but lower loadings for educators and parents (0.442), and a negative loading for young digital citizens (−0.305), resulting in a moderately strong loading of 0.584 for the combined demographics. Similarly, loadings for the Education and Awareness (EA) construct were mostly above the significance threshold, except for item ea1 for young digital citizens (0.543) and item ea2 for parents and educators (0.551). Items for the Parental Data Sharing (PDS) construct showed robust loadings across all four groups, notably, item pds2 for the combined demographics having a very high loading of 0.979. In the Perceived Risks and Benefits (PRB) construct, item prb1 had high loadings for AI professionals (0.947) and the combined demographics (0.911) but lower values for young digital citizens (0.489) and parents and educators (−0.142). Item prb2 had a low loading for AI professionals (0.422) but significant loadings for all other groups. For the Trust and Transparency (TT) construct, item tt1 showed low loadings for parents and educators (0.338) and young digital citizens (−0.510), while item tt2 had an exceptionally low loading of 0.082 for the combined demographics.

Despite the variability in factor loadings across the groups, all items and constructs were included in the analysis to capture the diverse perspectives of the participants. These variations suggest constructs may be interpreted or responded to differently, but each group highlights the need for further investigation to better understand the differences. More vigorous methods are needed to confirm any causal relationships.

2) CONSTRUCT RELIABILITY AND VALIDITY

We assessed convergent validity for each construct by calculating Average Variance Extracted (AVE) and Composite Reliability (CR) across the four groups: young digital citizens, parents and educators, AI professionals, and combined (see Table 5). AVE should exceed 0.50, indicating the hypothesized construct captures 50% of the variance in the items, and CR should also be above 0.75 [55]. For Data Ownership and Control (DOC), AI professionals showed acceptable values (AVE 0.550; CR 0.785), while all other groups were below acceptable levels. Results for Education and Awareness (EA) were mostly above the acceptable range, except for parents and educators with an AVE of 0.442 and a CR of 0.69. Parental Data Sharing (PDS) scores for AVE and CR exceeded the recommended levels across all four groups. The AVE for Perceived Risks and Benefits (PRB) was acceptable for all groups; however, the corresponding CR for young digital citizens (0.707), parents and educators (0.418), and AI professionals (0.669) all fell below 0.75. AVE and CR scores for Trust and Transparency (TT) struggled across all four groups, except for AI professionals (AVE 0.545; CR 0.757), which suggests that it did not capture significant variance to converge into a single construct. These findings underscore variability in construct validity, highlighting areas for potential refinement.

Results for the calculated rho_A values (Dillon-Goldstein's rho) are also in Table 5. The rho_A assesses the internal consistency and reliability of each measure; it evaluates the consistency of responses within the scale and is considered a more reliable measure than Cronbach's alpha [56]. Similar to the results for AVE and CR, the rho_A values vary across constructs and groups. For DOC, rho_A values are below the recommended 0.70 for all groups, indicating issues with sufficient internal consistency. EA demonstrates a strong internal consistency among young digital citizens (0.809), moderate internal consistency for AI professionals (0.625), and combined demographics (0.659), but very low consistency for educators and parents (0.376). PDS shows relatively high consistency across all four groups; however, the combined demographics group scored above the acceptable range (1.568), which indicates significant variation within the compounded response items. PRB had more mixed results, with only the combined group reaching acceptable levels (0.837). Finally, TT had values below the desired threshold for all groups except AI professionals (0.741). The low rho_A, in addition to the low CR and AVE values for TT across most groups, indicates a lack of consistency and insufficient variance captured by the construct. This suggests that TT may not be an effective measure for the intended concept and could require revisions to improve reliability and validity.

C. STRUCTURAL MODELS

To begin our Structural Equation Modeling (SEM) analysis, we built the model for the general population and applied it to four subgroups: young digital citizens (aged 16-19), parents and educators, AI professionals, and the combined populations. We described the model by looking at coefficients of determination (R^2's), path coefficients (β's), and corresponding p-values. The R^2 values determine the variance of a given construct by its antecedents, the β determines the strength of the relationship between constructs, and the p-values determine the statistical significance. By Chin's guidelines [43], [57], a β should be at least 0.2 to be considered relevant. Additionally, a model is considered statistically somewhat significant (*p) with a p-value < 0.1, quite significant (**p) with a p-value < 0.01, and highly significant (***p) with a p-value < 0.001 [43], [57]. Tables 6-9 present the standardized coefficients (β), t-statistics, and p-values for the model for young digital citizens, parents and educators, AI professionals, and combined demographics. Fig 3-6 presents the structural models for the four groups illustrating the causal relationships 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 explores direct, indirect and total effects among these constructs.

To align with the research questions (RQs), the findings are organized into sections that address each RQ and its associated hypotheses. This breakdown allows for a focused exploration of how perceived risks, perceived benefits, trust in AI systems, privacy management strategies, and ethical and contextual factors influence data-sharing behaviors across

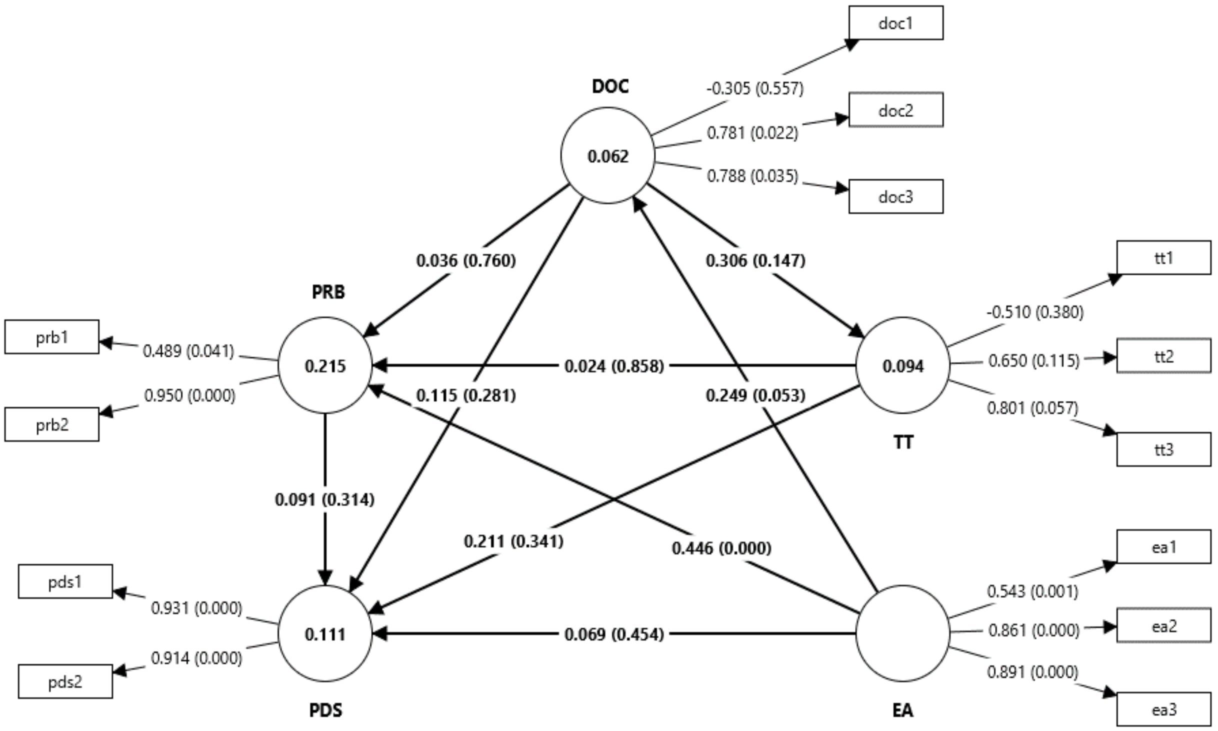


FIGURE 3. Model with direct effects for young digital citizens.

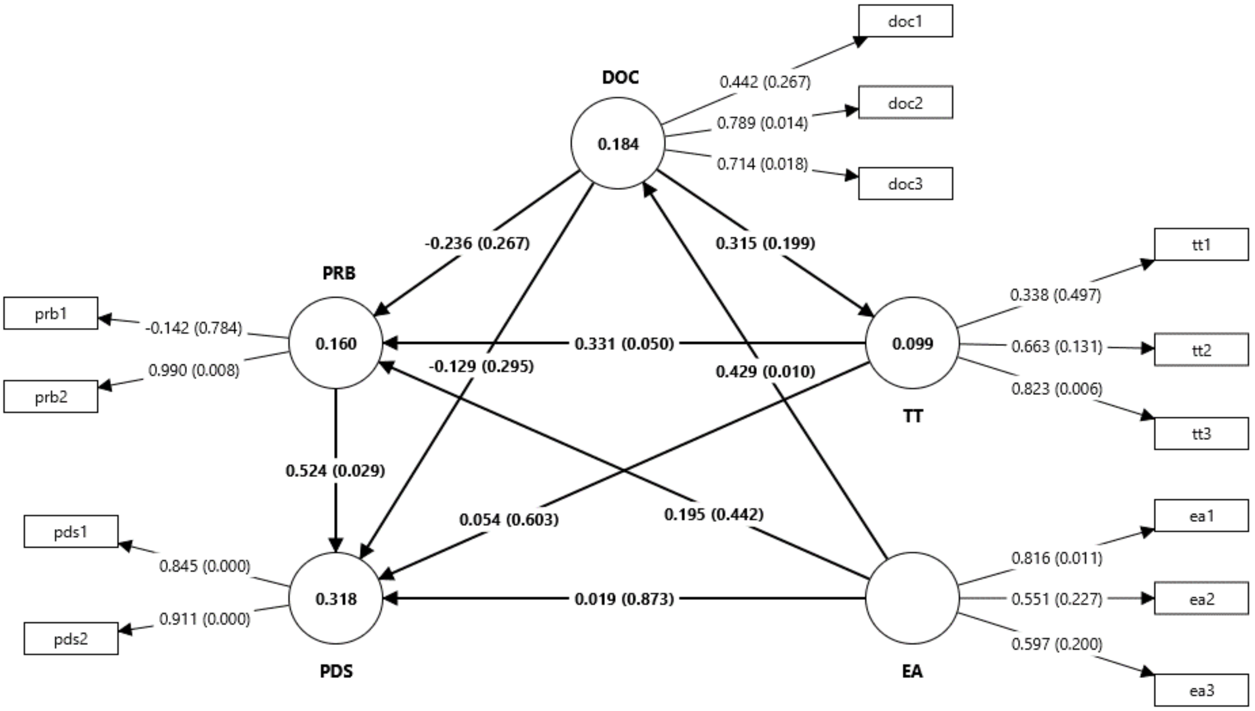


FIGURE 4. Model with direct effects for parents and educators.

the four subgroups. The results are presented in a structured manner, with each section highlighting the key findings relevant to the corresponding RQ.

1) PERCEIVED RISKS

RQ1 examines how perceived risks influence youths' and stakeholders' perceptions of data ownership and control

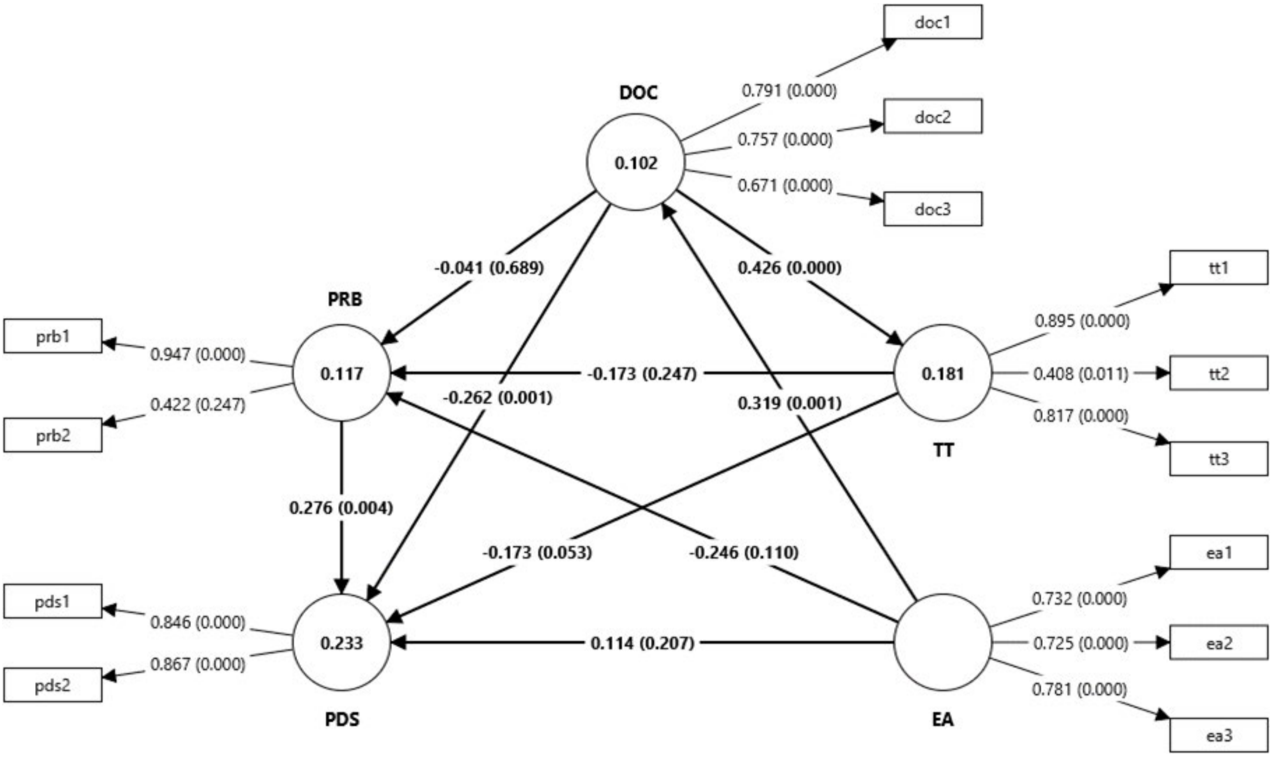


FIGURE 5. Model with direct effects for AI professionals.

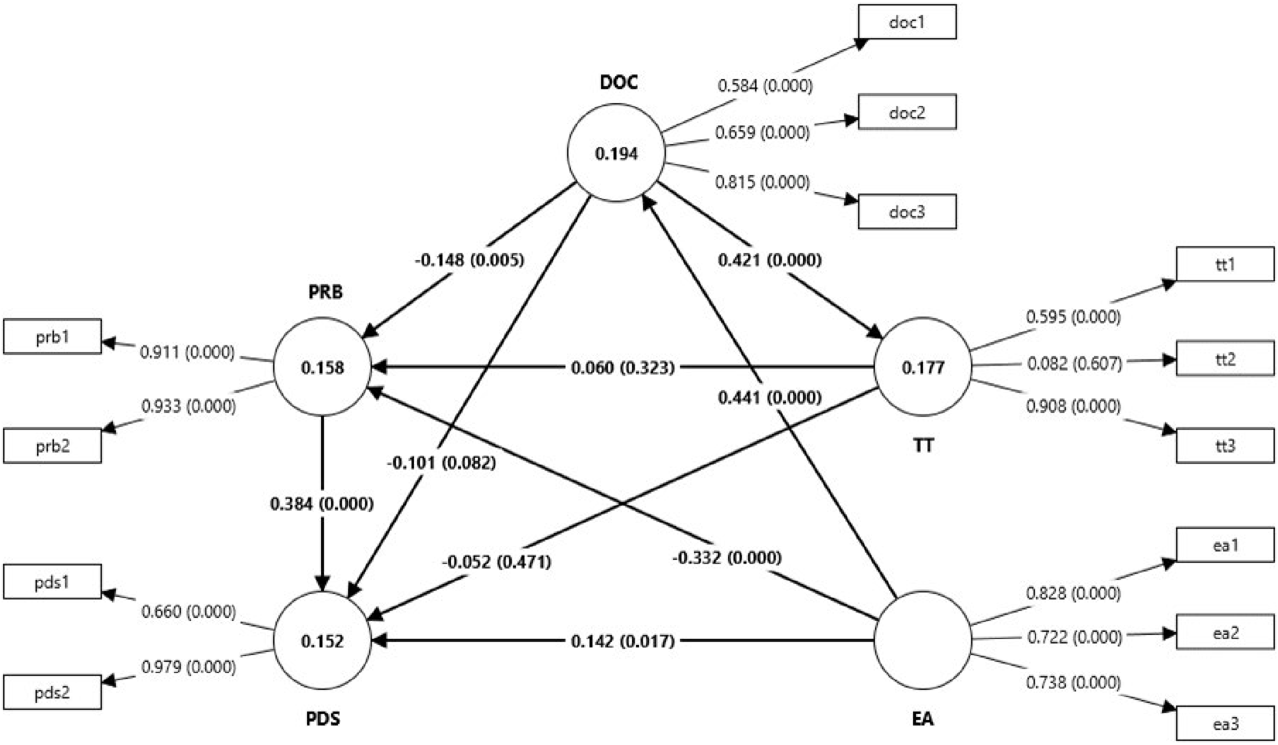


FIGURE 6. Model with direct effects for combined demographics.

in youth data-disclosure decisions. For young digital citizens, Fig. 3 shows that DOC had no significant effect on PDS ($\beta = 0.115$; p $>$ 0.1), leading to the rejection of H1. Similarly, PRB did not significantly mediate the relationship between DOC and PDS ($\beta = 0.003$; $p > 0.1$), resulting in the rejection of H2. For parents and educators, DOC also had no significant effect on PDS ($\beta = -0.129$; $p > 0.1$), and PRB did not mediate this relationship ($\beta = -0.124$; $p > 0.1$), leading to the rejection of H1 and H2. For AI professionals, DOC had a significant negative effect on PDS ($\beta = -0.262$; $p < 0.01$), supporting H1, but PRB did not mediate this relationship ($\beta = -0.011$; $p > 0.1$), rejecting H2. For the combined demographics, DOC had a significant negative effect on PDS ($\beta = -0.101$; $p < 0.1$), supporting H1, and PRB had a significant negative mediating effect between DOC and PDS ($\beta = -0.057$; $p < 0.01$), supporting H2. These findings suggest that perceived risks influence data ownership and control differently across groups, with significant effects observed for AI professionals and the combined group. The summarization of the hypothesis validation can be seen in Table 10.

2) PERCIEVED BENEFITS

RQ2 explores how perceived benefits shape youths' willingness to share personal information and parents' willingness to share their children's data. For young digital citizens, PRB had no significant effect on PDS ($\beta = 0.091$; $p > 0.1$), leading to the rejection of H4, and no significant mediating effect between TT and PDS ($\beta = 0.002$; $p > 0.1$), rejecting H7. For parents and educators, Fig. 4 shows that PRB had a moderately significant positive effect on PDS ($\beta = 0.524$; $p < 0.1$), supporting H4, but no significant mediating effect between TT and PDS ($\beta = 0.174$; $p < 0.1$), rejecting H7. For AI professionals, PRB had a significant positive effect on PDS ($\beta = 0.276$; $p < 0.01$), supporting H4, but no significant mediating effect between TT and PDS ($\beta = -0.048$; $p > 0.1$), rejecting H7. For the combined demographics, PRB had a significant positive effect on PDS ($\beta = 0.384$; $p < 0.001$), supporting H4, and was not found to have a significant indirect effect between TT and PDS ($\beta = -0.022$; $p > 0.1$), rejecting H7. These results indicate that perceived benefits play a key role in shaping data-sharing behaviors, particularly for parents and AI professionals. For a comprehensive overview of the hypothesis validation, refer to Table 10.

3) TRUST IN AI SYSTEMS

RQ3 investigates how transparency and trust in AI systems affect youth's decisions to disclose personal data. For young digital citizens, TT had no significant effect on PDS ($\beta = 0.211$; $p > 0.1$), leading to the rejection of H3, but DOC had a significant positive effect on TT ($\beta = 0.306$; $p < 0.1$), supporting H8. Additionally, TT did not significantly mediate the relationship between DOC and PDS ($\beta = 0.065$; $p > 0.1$), rejecting H10. For parents and educators, TT had a significant effect on PDS ($\beta = 0.054$; $p > 0.1$), and DOC also had no significant effect on TT ($\beta = 0.315$; $p > 0.1$), leading to the rejection of H3 and H8. Furthermore, TT did not significantly mediate the relationship between DOC and PDS ($\beta = 0.017$; $p > 0.1$), leading to the rejection of H10. For AI professionals, as shown in Fig. 5, TT had a moderately negative effect on PDS ($\beta = -0.173$; $p < 0.1$), supporting H3, and DOC had a significant positive effect on TT ($\beta = 0.426$; $p < 0.001$), supporting H8. TT had a moderately significant mediating effect between DOC and PDS ($\beta = -0.074$; $p < 0.1$), supporting H10. For the combined demographics, DOC had a significant positive effect on TT ($\beta = 0.421$; $p < 0.001$), supporting H8, but TT had no significant effect on PDS ($\beta = -0.052$; $p > 0.1$), rejecting H3. Additionally, TT did not significantly mediate the relationship between DOC and PDS ($\beta = 0.023$; $p > 0.1$), leading to the rejection of H10.. These findings highlight the varying role of trust and transparency across groups. The results of the hypothesis validation are summarized in Table 10.

4) PRIVACY MANAGEMENT STRATEGIES

RQ4 examines how youth and parents manage boundaries when interacting with AI technologies. For young digital citizens, DOC had no significant effect on PRB ($\beta = 0.036$; $p > 0.1$), leading to the rejection of H5, and TT had no significant effect on PRB ($\beta = 0.024$; $p > 0.1$), rejecting H9. For parents and educators, DOC also had no significant effect on PRB ($\beta = -0.236$; $p > 0.1$), rejecting H5, but TT had a significant effect on PRB ($\beta = 0.331$; $p < 0.1$), supporting H9. For AI professionals, DOC had no significant effect on PRB ($\beta = -0.041$; $p > 0.1$), rejecting H5, but TT had a moderately negative effect on PDS ($\beta = -0.173$; $p < 0.1$), supporting H9. For the combined demographics, Fig. 6 shows that DOC had a significant negative effect on PRB ($\beta = -0.148$; $p < 0.01$), supporting H5, and TT had no significant effect on PRB ($\beta = 0.060$; $p > 0.1$), rejecting H9. These results suggest that privacy management strategies vary across groups, with stronger effects observed for AI professionals and the combined group. Table 10 presents a summary of the hypothesis validation findings.

5) ETHICAL AND CONTEXTUAL FACTORS

RQ5 explores how education and awareness about AI impact youths' sense of control and autonomy. For young digital citizens, EA had a significant positive effect on PRB ($\beta = 0.446$; $p < 0.001$), supporting H6, and a moderately positive effect on DOC ($\beta = 0.249$; $p < 0.1$), supporting H13. However, EA had no significant effect on PDS ($\beta = 0.069$; $p > 0.1$), rejecting H11, and no significant total effect on TT ($\beta = 0.076$; $p > 0.1$), rejecting H12. Additionally, PRB did not significantly mediate the relationship between EA and PDS ($\beta = 0.040$; $p > 0.1$), leading to the rejection of H14. For parents and educators, EA had a moderately positive effect on DOC ($\beta = 0.429$; $p < 0.1$), supporting H13, but no significant effect on PRB ($\beta = 0.195$; $p > 0.1$), rejecting H6, and no significant total effect on TT ($\beta = 0.135$; $p > 0.1$), rejecting H12. Furthermore, PRB did not significantly mediate the relationship between EA and PDS ($\beta = 0.102$; $p > 0.1$), leading to the rejection of H14. For AI professionals, EA had a significant positive effect on DOC

($\beta = 0.319$; $p < 0.01$), supporting H13, and a significant total effect on TT ($\beta = 0.136$; $p < 0.01$), supporting H12. However, EA has no significant effect on PRB ($\beta = -0.246$; $p > 0.1$), rejecting H6, and no significant effect on PDS ($\beta = 0.114$; $p > 0.1$), rejecting H11. Additionally, PRB did not significantly mediate the relationship between EA and PDS ($\beta = -0.068$; $p > 0.1$), leading to the rejection of H14. For the combined demographics, EA had a significant positive effect on DOC ($\beta = 0.441$; $p < 0.001$), supporting H13, and a significant total effect on TT ($\beta = 0.186$; $p < 0.001$), supporting H12. PRB had a significant negative mediating effect between EA and PDS ($\beta = -0.128$; $p < 0.001$), supporting H14. However, EA has no significant effect on PDS ($\beta = 0.142$; $p > 0.1$), rejecting H11. These findings highlight the complex role of education and awareness in shaping privacy perceptions and behaviors. The hypothesis validation outcomes are consolidated and presented in Table 10.

D. QUALITATIVE FINDINGS

In addition to the quantitative analysis, qualitative data were gathered to capture respondents' subjective perspectives on privacy concerns related to AI tools and data sharing. As part of an online survey, each demographic group (young digital citizens, parents and educators, and AI professionals) received three open-ended questions linked to the five primary research questions (RQ1–RQ5) [58]. The wording was slightly adjusted for each demographic group to reflect each group's relation to young digital citizens, as shown in Table 11. We further supplemented the survey data with one-on-one interviews conducted with parents, educators, and AI professionals, as well as two focus groups-one with parents and educators, and another with AI professionals (conducted virtually using Microsoft Teams). This multi-layered qualitative approach was designed to enrich and complement the quantitative findings, providing a deeper, more nuanced understanding of how different stakeholder groups perceive and navigate privacy issues in AI contexts. The insights gathered were then analyzed to systematically address the study's core research questions, as outlined in the next section.

1) INFLUENCE OF PERCEIVED RISKS ON DATA OWNERSHIP AND CONTROL (RQ1)

Across all groups, concerns about loss of control, data misuse, and surveillance emerged as primary risks influencing youths' and stakeholders' views on data ownership and control (DOC). Many youth respondents expressed discomfort over uncertainty regarding data ownership, emphasizing that once shared, personal data is no longer within their control. As one youth participant stated, "I am mainly concerned about what data is being taken and how it is used, as I feel we often aren't informed clearly about what data is being taken and used" (S-YDC #5). Another highlighted fears of data resale, saying, "My data could be sold without my knowing who it's going to" (S-YDC #107). These concerns align with the quantitative findings, where DOC showed a lower mean score among youth (3.42) compared to AI professionals (3.95) and parents/educators (3.75), suggesting weaker confidence in personal data control among younger users.

Surveillance and profiling by AI systems were also widely cited as major risks. Many youth respondents worried about AI's ability to track and infer personal details, even beyond explicit data-sharing. One participant shared, "I feel uncomfortable knowing AI can recognize my face in public places" (S-YDC #93), while another feared, "AI will guess everything about us. Sensitive topics I research could be recorded forever; voice assistants may listen in when I am just hanging out" (S-YDC #84). Similarly, AI professionals echoed these risks, with one stating, "Users may not realize how much of their data is being captured. AI could unintentionally memorize personal details from its users" (S-AIP #116). These findings reinforce the structural model results, which showed a negative relationship between DOC and Perceived Risks and Benefits (PRB) ($\beta = -0.148$, $p < 0.01$) in the combined demographic analysis, indicating that as privacy concerns increase, users feel less in control of their data.

Parents and educators placed greater emphasis on the lack of youth awareness in data-sharing decisions, arguing that uninformed sharing exacerbates privacy risks. One parent remarked, "I am concerned about the misuse and manipulation of the data they share. I also think that most young people are unaware or apathetic about AI systems and their potential for misuse" (S-PE #17). Another educator noted, "Many children and adolescents will use AI without considering their own privacy (similar to how many use social media)" (S-PE #40), suggesting that privacy education is critical for fostering a stronger sense of DOC. This aligns with the Education and Awareness (EA) construct, which showed a significant positive effect on DOC ($\beta = 0.441$, $p < 0.001$) in the combined dataset, highlighting the role of education in mitigating perceived risks.

AI professionals provided technical insights into privacy vulnerabilities, particularly regarding data leakage through AI models. One researcher explained, "AI might accidentally recreate sensitive data from its training sets, exposing private information" (S-AIP #85), raising concerns about long-term data retention and unintended exposure. Another stated, "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), reinforcing broader concerns about the opacity of AI-driven data processing. A summary of trends discussed in this section can be seen in Table 12.

2) ROLE OF PERCEIVED BENEFITS IN DATA-SHARING DECISIONS (RQ2)

Participants identified several perceived benefits of AI systems using personal data, with the most frequently mentioned advantage being its role in education. Many young digital citizens reported using AI tools for academic purposes, describing them as helpful while expressing caution about sharing personal data. One youth stated, "I use them to help me with homework or chat for fun but try not to share personal stuff. It's super helpful'' (S-YDC #15), while another shared a similar perspective: ''I just use ChatGPT for homework and stuff, but I don't share personal things. I think it's super helpful, but I try not to rely on it too much'' (S-YDC #9).

Educators reinforced this viewpoint, emphasizing AI's potential to reduce mundane tasks and enhance students' learning experiences. One educator noted, ''I think on one hand they can be treated as just another tool that can potentially be used to, you know, reduce mundane workload and let students work on more interesting and challenging parts of, you know, work in our discipline'' (I-Educator #1). Others highlighted AI's ability to personalize learning, accommodate different learning styles, and provide accessibility features for students with disabilities. Another educator explained, ''We were just talking about personalizing learning for students having different needs or different paces of learning. That's one positive side of AI tools or AI systems being complemented in the education system. There are some AI tools out there which anonymize the data to tailor learning experiences. So that kind of reduces the risk somewhat. So student privacy is maintained. And learning is also personalized for the students' need. So that's a positive of using AI in education'' (FG1-Educator #4).

While youth, parents, and educators primarily viewed AI through an educational lens, AI professionals took a broader view, focusing on AI's ability to enhance personalization and efficiency across multiple sectors. One AI developer described the advantages of AI-driven personalization: ''Talking about benefits of sharing data with AI systems, I would say they are amazing. Quite amazing, as far as it comes to me, for an example. One of the biggest boons [sic], I would say that comes with sharing data with an AI system is that you get personalized services. So basically, AI can analyze your personal data to provide highly tailored services'' (FG2-Developer #4).

One developer emphasized AI's efficiency and error reduction capabilities in software development, stating, ''It would make the application development much faster than the traditional coding methods. It could automate repetitive tasks, generate code snippets, and even provide helpful suggestions, allowing myself and developers to concentrate on high-level design and functionality. So efficiency was one of the key reasons for us picking AI. [It] not only speeds up the development but also reduces the likelihood of human error, which can in turn lead to developing more reliable applications'' (FG2-Developer #6). A summary of the stakeholders' perspectives on the benefits of AI systems can be found in Table 13.

3) IMPACT OF TRANSPARENCY AND TRUST ON DISCLOSURE DECISIONS (RQ3)

Across all stakeholder groups, participants expressed significant privacy concerns regarding AI systems, primarily citing a lack of transparency and limited user control over data-sharing practices. However, the way these concerns manifested varied among young digital citizens, parents/educators, and AI professionals.

Young digital citizens frequently described their uncertainty about what data is collected and how it is used, with many stating that privacy policies were unclear or difficult to understand. One youth commented, ''I do not know enough about them to be concerned about what I should be concerned about'' (S-YDC #2), while another expressed frustration over the lack of transparency, stating, ''I am mainly concerned about what data is being taken and how it is used, as I feel we often aren't informed clearly about what data is being taken and used'' (S-YDC #5). Others highlighted the complexity of AI privacy settings, with one respondent noting, ''I shouldn't have to be a tech expert to keep my info private'' (S-YDC #62), and another adding, ''I feel like my privacy depends on settings I barely understand'' (S-YDC #48). Additionally, some youth raised concerns about international data sharing and regulatory differences, questioning, ''What if my data is shared with companies overseas, beyond my country's laws?'' (S-YDC #132).

Parents and educators echoed many of these concerns but also emphasized the long-term implications of data collection on youth development and safety. One educator criticized the lack of regulatory oversight, stating, ''I do not trust that information gathered by AI will be used presently or in the future in an informed manner for the benefit of the individual, but rather fear its exploitation on both an individual and mass level. Guardrails and safety mechanisms to protect people barely exist, people do not know enough about what is being gathered and how it is being used, and very few mechanisms exist to inform them'' (S-PE #10). Others worried about how AI-driven profiling could shape young users' experiences and influence their behavior, with one parent expressing concern over ''psychological profiling of student's attitudes and beliefs for manipulation and propaganda purposes. Fortune 500 companies sharing this data with government for authoritarian, non-democratic purposes'' (S-PE #20). Another parent specifically noted concerns regarding children's safety in digital spaces, stating, ''I'm mostly worried about how much personal information these AI systems collect about my child and what they do with it. I don't feel like I have control over the data, or know if we can remove it. I also worry about my children's safety online and if AI makes them more exposed to things like cyberbullying'' (S-PE #31).

AI professionals focused on the technical risks of AI privacy practices, particularly emphasizing the difficulty of opting out of data collection and the long-term retention of personal information. One AI researcher pointed out the lack of accessible data controls, stating, ''Saying NO to data collection isn't always clear or easy, and opting out can mean missing out on useful features'' (S-AIP #57). Others expressed concerns over AI systems inadvertently retaining and exposing sensitive information, explaining, ''There is a risk that the model could inadvertently generate or expose private information it learned from its training data'' (S-AIP #77) and ''Neural networks might store patterns that include sensitive info from users. Once trained, that data can be hard to fully remove or control'' (S-AIP #122). Cybersecurity risks were also a major theme, with one respondent stating, ''If AI systems keep data longer than needed, it is more at risk of being hacked or misused'' (S-AIP #48).

Ultimately, participants across all groups stressed that a lack of transparency and clear user controls contributes to mistrust in AI-driven data collection. One AI professional summarized these concerns, stating, ''AI systems often rely on a huge amount of data including personal/sensitive data; think about smart assistants, recommendation engines, or health apps. The problem? This data can be misused, hacked, or even just over-collected. Machine learning models can also make decisions that feel invasive or less accurate because it's trained on data that may not always represent everyone fairly'' (S-AIP #103). A summary of participants' responses to privacy concerns in AI systems can be found in Table 14.

4) BOUNDARY MANAGEMENT STRATEGIES IN AI INTERACTIONS (RQ4)

Participants across all demographic groups identified various strategies and measures to enhance privacy protections in AI systems, focusing on platform-level changes, regulatory protections, and user education. However, distinct differences emerged between young digital citizens, parents and educators, and AI professionals in how they believed privacy should be managed.

Young digital citizens primarily advocated platform-level improvements, expressing a need for clearer privacy settings, ongoing consent mechanisms, and greater transparency in data usage. One participant emphasized the importance of making privacy settings more accessible, stating, ''Make privacy options super clear and right in front when I install an app'' (S-YDC #67). Others similarly urged AI platforms to provide straightforward options to adjust privacy settings, with one stating, ''Give us clear options to adjust privacy settings and control what data we share'' (S-YDC #25), while another pointed out that existing platforms often obscure such options, stating, ''Don't hide privacy settings behind complicated menus'' (S-YDC #38).

Beyond controls, several participants stressed the need for greater transparency in how AI systems utilize personal data, with one requesting, ''Clearer definitions and explanations of how data is being used and why/where'' (S-YDC #5), and another suggesting, ''Let us see a history of how our data has been used'' (S-YDC #97).

In addition to platform-based changes, many youth participants highlighted the importance of legal and regulatory measures to enforce privacy protections. Some called for strict penalties for companies that fail to comply with privacy standards, such as ''Mandatory guidelines they must abide by, with the company being punishable with major fines from a governing body'' (S-YDC #3). Others proposed global privacy frameworks to ensure consistent protections across different jurisdictions, with one stating, ''Develop global standards for data privacy protections'' (S-YDC #107). Additional suggestions included privacy certification for applications, such as, ''Create a certification for apps with great privacy standards'' (S-YDC #112), and mandatory transparency disclosures, such as, ''Make it mandatory for apps to show how they secure our information'' (S-YDC #147).

Another prominent theme among youth responses was the need for increased privacy education. Many suggested integrating digital privacy awareness into school curricula, with one stating, ''Teach privacy basics in school so we know our rights'' (S-YDC #51), while another stressed the importance of online safety education, stating, ''Teach people how to manage privacy online'' (S-YDC #90). Some youth also highlighted the role of parents in privacy education, suggesting parental guidance tools for younger users while preserving autonomy, such as ''Give parents tools to guide younger kids' online safety but with some ethical restrictions'' (S-YDC #64). Others suggested that youth should actively participate in shaping AI privacy policies, with one recommending, ''Have youth councils help design privacy rules they actually understand'' (S-YDC #138).

Parents and educators largely echoed youth concerns but focused more on age-appropriate privacy controls and the role of parental oversight. Many respondents supported more granular controls for both youth and parents, with one explaining, ''There should be clarity on the purpose of personalized data being shared. Young people should have access to control their actions accordingly'' (S-PE #13). Another participant emphasized the need for clear parental controls and complete opt-out options, stating, ''More controls as well as an explanation of how all data is used. The controls should include a complete opt-out option as well as selections or options for which data can be shared or used'' (S-PE#12). Some parents specifically emphasized parental control over AI-driven applications for children, with one parent explaining, ''I think AI-based tools for kids need to be a lot safer and clearer. It should be easy to know what the AI tool is doing with my kid's information and why it needs it. These tools shouldn't collect more data than they really need. Parents should be able to control or delete that data if we want'' (S-PE #31).

In contrast to youth respondents, parents and educators placed greater emphasis on regulatory interventions, particularly those aimed at age-based privacy restrictions. Some called for mandatory educational programs prior to AI usage, with one educator suggesting, ''First and foremost, AI should not be accessible to simply anyone. Before given access to AI, students need to be informed of the risks of sharing personal information online'' (S-PE #40). Others proposed specialized youth data protection laws, such as, ''Youth-centric privacy laws'' (S-PE #79), or banning the monetization of youth data, with one stating, ''Monetization of data about young people should not be allowed. If collected, data should only be used in aggregate and anonymized ways, without profiling any one user'' (S-PE #78).

Similar to youth respondents, parents and educators emphasized the importance of digital privacy education, though they also stressed educating adults, including teachers and parents, about AI privacy. One parent recommended introducing privacy education in schools from an early age, stating, "I think that young people should be educated, probably around Grade eight or nine, about how their data is being collected and used" (S-PE #17). Another suggested expanding privacy awareness beyond schools, stating, "Awareness campaigns in schools and colleges" (S-PE #19).

Interestingly, several parents and educators also noted that adults themselves lack sufficient knowledge about AI privacy, with one explaining, "It's important to educate everyone on protecting their privacy when using online AI tools. Educators, in particular, should never use their students' identities on these platforms. Schools and companies also have a responsibility to make sure student data is securely stored and only shared with proper consent" (S-PE #94). Another parent supported the idea of adult-oriented AI privacy education, recommending, "Proper literacy programs to educate parents about it" (S-PE #114). One respondent referenced existing European privacy frameworks as a model for improvement, stating, "We need something more along the EU GDPR + AI Act for protecting privacy and enforcing meaningful fines for infractions. AI should be part of a coherent, comprehensive curriculum around digital skills—much like Action 6 of the EU Digital Education Action Plan" (S-PE #76).

AI professionals largely echoed concerns shared by other stakeholders but emphasized technical solutions such as anonymization, encryption, and federated learning. One developer outlined several privacy-enhancing techniques, stating, "To enhance privacy in AI systems, I would focus on anonymizing data and using differential privacy to protect individual information. Implementing federated learning can help keep data on local devices. Encryption is essential for securing data at rest and in transit" (S-AIP #7). Similarly, others highlighted technical strategies to restrict personal data collection, with one explaining, "Anonymization and pseudonymization are essential techniques for protecting personally identifiable information (PII) and sensitive data in AI systems" (S-AIP #16), while another recommended, "Use differential privacy, homomorphic encryption, or similar technologies to remove personally identifiable information to safeguard user identities" (S-AIP #29). Although AI professionals supported greater transparency, few explicitly mentioned regulatory or legal interventions. Instead, they focused on platform-driven protections, such as "Straightforward, accessible privacy policies to explain data practices" (S-AIP #25) and user-accessible data logs, as one participant suggested, "Give users an easy way to see exactly what data an AI has about them, so they know what's being used" (S-AIP #52). A considerable number of AI professionals also emphasized education as a key privacy protection strategy, particularly in making AI more understandable for youth users. One researcher stated, "Teach young people about digital privacy early, so they know how to make smarter choices online" (S-AIP #127), while another suggested, "Games or apps could even teach these skills while being fun" (S-AIP #130). A summary of the proposed privacy measures is outlined in Table 15.

5) EFFECTS OF EDUCATION AND AWARENESS ON DATA CONTROL AND AUTONOMY (RQ5)

Across all three demographic groups, participants discussed various approaches to balancing the benefits of AI-driven data usage with privacy protection. Youth respondents primarily focused on individual privacy management strategies, including using privacy-focused tools such as VPNs, ad-blockers, and encrypted messaging apps. One youth explained, "I run ad-blockers or privacy extensions in my browser to limit hidden tracking" (S-YDC #72), while another mentioned, "I download privacy-focused apps like secure browsers or VPNs" (S-YDC #125). Other participants preferred selective data sharing, sharing only necessary information to minimize risks. One respondent described, "I only share data when it really adds value" (S-YDC #40), while another explained, "I only provide information when it's necessary and always check privacy settings on apps" (S-YDC #29). Some youth highlighted the importance of transparency, emphasizing that platforms should offer more clarity regarding data collection. One participant stated, "Let me see a before-and-after picture: what's different if I share less?" (S-YDC #59), while another added, "Tell me how using my data benefits me, not just the company" (S-YDC #38).

Parents and educators emphasized education and awareness as key to enabling informed privacy decisions for young users. Many stressed the need for privacy education in schools to help students understand the risks of AI-driven data collection. One educator explained, "I try to inform students so they can better be informed about their use of AI, and see the trade-off they are making when they use the (obvious) benefits. I try to tell myself too. And I teach them about ways to safeguard their identity information while using AI, though that is very challenging" (S-PE #5). Other educators similarly noted, "I warn students to be aware of where they put their private information; and I teach them to be aware of the source of the information they are getting" (S-PE #7). Some parents actively educate their children about privacy risks, with one parent sharing, "We need to make sure our children use tools that don't ask for too much personal information. I teach my kids not to share all of the personal and private content online" (S-PE #115). Others emphasized direct parental control over AI interactions, with one explaining, "Family discussions about social media algorithms, computer game design, YouTube and Snapchat video feeds. Social media is not allowed (messaging and email is allowed), Internet browsers are used in school or with some parental supervision and time limits outside of school" (S-PE #18).

AI professionals approached the issue from a technical and policy perspective, advocating for user-controlled privacy settings, strong encryption, and data anonymization. Many supported privacy-preserving AI development, with one researcher explaining, ''I prioritize using data that's been anonymized or synthetically generated to protect privacy'' (S-AIP #73). Others discussed multi-layered approaches that integrate regulatory compliance, data minimization, and transparency mechanisms to ensure user autonomy, stating, ''Balancing data usage and privacy is challenging. In my work, I prioritize using only the necessary data and implement privacy-preserving techniques like anonymization and encryption. We often collaborate with legal and compliance teams to ensure we are meeting regulations'' (S-AIP #7). Additionally, AI professionals supported clear and accessible privacy controls, with one developer recommending, ''Make sure users have options to decide what data they want to share, and under what conditions'' (S-AIP #46), while another emphasized the importance of informed consent, explaining, ''Use clear interfaces for privacy controls so users know exactly what's happening. When asking for consent, make sure it's straightforward, no long, unreadable policies'' (S-AIP #133). AI professionals also acknowledged the challenges of maintaining privacy in AI systems, with one noting, ''Despite best efforts, privacy lapses can happen due to shortcuts or lack of adherence to best practices. I think it's an ongoing effort to keep privacy at the forefront while still delivering effective solutions'' (S-AIP #7). A summary of participants' responses is provided in Table 16.

V. DISCUSSION

A. STRENGTHENING PRIVACY MANAGEMENT THROUGH EDUCATION AND AWARENESS

The cornerstones of preparing young digital citizens with the information and abilities needed to protect their privacy in AI-driven settings are education and awareness (EA). EA's important role in encouraging proactive privacy behaviors is highlighted by its strong impact on promoting Data Ownership and Control (DOC) ($\beta = 0.249$, p = 0.053). Disparities in digital literacy, especially among parents and educators (AVE = 0.442), however, highlight a lack of knowledge about AI's data practices, which may make it more difficult for them to help young people make wise decisions. This can be addressed by methodically incorporating privacy education into school curricula, emphasizing AI-specific threats such as behavioral tracking, algorithmic decision-making, and data profiling. Public awareness campaigns can also be used to teach parents, teachers, and students about good privacy management practices. To create gamified platforms and interactive, scenario-based learning resources that make privacy education interesting and approachable, governments and tech firms must work together. Users may better understand their rights, reduce privacy threats, and confidently traverse AI environments by bolstering EA activities. To guarantee fair access to AI literacy, future studies should assess the long-term efficacy of privacy education initiatives across various socioeconomic and cultural backgrounds.

B. TRANSPARENCY AND TRUST AS ESSENTIAL PILLARS OF PRIVACY

Although it is still difficult to successfully include transparency and trust (TT) into AI governance, these concepts are essential for promoting responsible interaction with AI systems. Despite TT's proven favourable impact on Data Ownership and Control (DOC) ($\beta = 0.306$), the study's results highlight a crucial gap in AI transparency, as seen by its comparatively low AVE (0.395). Because users are still unsure of how their data is processed and used, the ambiguity around AI data-handling procedures makes them reluctant to share information. AI systems must provide easily understandable explanations of data usage guidelines and privacy settings to increase confidence. Consent-based data-sharing models, explainable AI (XAI) interfaces, and real-time privacy dashboards are a few examples of features that can help consumers make wise choices. Mandating transparency audits and compelling AI developers to give comprehensive yet understandable data policies are two further ways that ethical governance frameworks should strengthen accountability. Furthermore, AI systems need to be made to adapt to different degrees of digital literacy so that even non-technical people and younger users can easily traverse privacy settings. To ascertain how transparency-driven treatments affect privacy attitudes over time, future research should examine the long-term effects of trust-enhancing tactics on user involvement, especially among teens.

C. ENHANCING DIGITAL LITERACY FOR PROACTIVE PRIVACY MANAGEMENT

A key component of proactive privacy management is digital literacy, which helps people connect the dots between theory and practice while using AI-powered systems. Although the study shows a strong correlation between Data Ownership and Control (DOC) and Education and Awareness (EA), there are still notable differences in digital literacy among various stakeholder groups. The AVE ratings for EA were notably lower for parents and educators (0.442), suggesting gaps in their capacity to successfully mentor young people in privacy-related decision-making. Targeted interventions are needed to address this, including interactive workshops, organized digital literacy programs, and privacy training tailored to AI. Learning about privacy may be made more interesting and approachable by using techniques like interactive simulations, gamified privacy education resources, and community-driven awareness campaigns. Additionally, lowering disparities and promoting an inclusive AI ecosystem where all users can confidently handle privacy challenges depends on giving marginalized communities priority when it comes to digital literacy. For young digital citizens to be prepared to assess the risks of data sharing and protect their personal information, policymakers and educators should concentrate on incorporating AI-specific digital literacy into school curricula. Future studies should examine scalable strategies for integrating digital literacy initiatives

TABLE 4. Exploratory factor analysis.

Construct	Item	Factor Loading			
		Young Digital Citizens	Parents & Educators	AI Professionals	Combined
DOC	doc1	-0.305	0.442	0.791	0.584
	doc2	0.781	0.789	0.757	0.659
	doc3	0.788	0.714	0.671	0.815
EA	ea1	0.543	0.816	0.732	0.828
	ea2	0.861	0.551	0.725	0.722
	ea3	0.891	0.597	0.781	0.738
PDS	pds1	0.931	0.845	0.846	0.660
	pds2	0.914	0.911	0.867	0.979
PRB	prb1	0.489	-0.142	0.947	0.911
	prb2	0.950	0.990	0.422	0.933
TT	tt1	-0.510	0.338	0.895	0.595
	tt2	0.650	0.663	0.408	0.082
	tt3	0.801	0.823	0.817	0.908

TABLE 5. Construct reliability and validity.

Construct	Young Digital Citizens			Parents & Educators			AI Professionals			Combined		
	rho_A	AVE	CR	rho_A	AVE	CR	rho_A	AVE	CR	rho_A	AVE	CR
DOC	0.449	0.441	0.488	0.428	0.443	0.694	0.599	0.550	0.785	0.498	0.480	0.731
EA	0.809	0.610	0.818	0.376	0.442	0.697	0.615	0.557	0.790	0.659	0.584	0.808
PDS	0.832	0.851	0.920	0.741	0.772	0.871	0.640	0.734	0.846	1.568	0.697	0.816
PRB	0.543	0.571	0.707	X	0.500	0.418	0.322	0.537	0.669	0.837	0.851	0.919
TT	0.389	0.442	0.346	0.332	0.410	0.653	0.741	0.545	0.767	0.398	0.395	0.581

into national curricula and evaluate how they affect privacy practices over the long run.

D. REDEFINING THE ROLE OF ETHICAL DESIGN IN AI SYSTEMS

Findings related to Transparency and Trust (TT) highlight the need for ethical AI design to handle the complex privacy issues raised by AI-driven systems. Although Data Ownership and Control (DOC) has a favourable effect on TT ($\beta = 0.306$), the comparatively low AVE for TT (0.395) indicates that consumers have trouble comprehending AI's privacy measures. Accessibility, inclusivity, and simplicity should be given top priority in ethical AI design to guarantee that even younger and less tech-savvy users can maintain their privacy. To increase user trust, developers must incorporate real-time transparency tools, adaptive privacy restrictions, and simple permission procedures. Furthermore, integrating ethical design principles into AI governance frameworks requires cooperation between technologists, legislators, and end users. While maintaining accountability for AI-driven decisions, AI designers should concentrate on developing privacy-by-design systems that give consumers more transparent data management choices. Future studies should concentrate on creating cross-sector ethical AI frameworks that guarantee equity, reduce algorithmic biases, and methodically assess how ethical AI design affects user engagement and trust over the long run.

E. BALANCING RISKS AND BENEFITS IN DATA SHARING

Users must carefully consider the benefits and possible risks of sharing data when making privacy decisions in AI ecosystems, as evidenced by the interaction between Education and

TABLE 6. Structural estimates (hypothesis testing) for young digital citizens.

Structural path	Direct effect			Total effect			Indirect effect		
	Std β	T	P	Std β	T	P	Std β	T	P
DOC → PDS	0.115	1.079	0.281	0.184	1.284	0.199			
DOC → PRB	0.036	0.305	0.760	0.043	0.354	0.723			
DOC → TT	0.306	1.451	0.147	0.306	1.451	0.147			
EA → DOC	0.249	1.934	0.053	0.249	1.934	0.053			
EA → PDS	0.069	0.749	0.454	0.155	2.115	0.035			
EA → PRB	0.446	4.666	0.000	0.457	5.790	0.000			
EA → TT				0.076	1.171	0.241			
PRB → PDS	0.091	1.008	0.314	0.091	1.008	0.314			
TT → PDS	0.211	0.953	0.341	0.213	0.996	0.319			
TT → PRB	0.024	0.179	0.858	0.024	0.179	0.858			
DOC → PRB → PDS							0.003	0.188	0.851
DOC → TT → PDS							0.065	0.835	0.404
EA → PRB → PDS							0.040	1.031	0.303
TT → PRB → PDS							0.002	0.106	0.916

TABLE 7. Structural estimates (hypothesis testing) for parents and educators.

Structural path	Direct effect			Total effect			Indirect effect		
	Std β	T	P	Std β	T	P	Std β	T	P
DOC → PDS	-0.129	1.047	0.295	-0.181	1.010	0.313			
DOC → PRB	-0.236	1.110	0.267	-0.132	0.567	0.571			
DOC → TT	0.315	1.284	0.199	0.315	1.284	0.199			
EA → DOC	0.429	2.568	0.010	0.429	2.568	0.010			
EA→ PDS	0.019	0.160	0.873	0.044	0.243	0.808			
EA → PRB	0.195	0.769	0.442	0.139	0.448	0.654			
EA → TT				0.135	1.179	0.238			
PRB → PDS	0.524	2.182	0.029	0.524	2.182	0.029			
TT → PDS	0.054	0.520	0.603	0.227	1.670	0.095			
TT → PRB	0.331	1.962	0.050	0.331	1.962	0.050			
DOC → PRB → PDS							-0.124	1.355	0.175
DOC → TT → PDS							0.017	0.429	0.668
EA → PRB → PDS							0.102	0.798	0.425
TT → PRB → PDS							0.174	1.841	0.066

Awareness (EA) and Perceived Risks and Benefits (PRB) ($\beta = 0.446$, $p < 0.001$). Users voice concerns about profiling, monitoring, and data breaches even as they recognize the advantages of AI, such as enhanced service accessibility and personalized learning experiences. AI systems must have tools that support risk-benefit analysis, such as adaptive consent procedures that offer contextualized explanations of the ramifications of sharing various sorts of data, to promote informed decision-making. To guarantee that people are not unintentionally exposed to high-risk data processing operations, AI governance should also place a strong emphasis on openness in the way user data is used. To enable

TABLE 8. Structural estimates (hypothesis testing) for AI professionals.

Structural path	Direct effect			Total effect			Indirect effect		
	Std β	T	P	Std β	T	P	Std β	T	P
DOC → PDS	-0.262	3.210	0.001	-0.367	4.495	0.000			
DOC → PRB	-0.041	0.400	0.689	-0.115	0.894	0.371			
DOC → TT	0.426	5.315	0.000	0.426	5.315	0.000			
EA → DOC	0.319	3.289	0.001	0.319	3.289	0.001			
EA → PDS	0.114	1.263	0.207	-0.071	0.834	0.405			
EA → PRB	-0.246	1.599	0.110	-0.283	2.181	0.029			
EA → TT				0.136	2.699	0.007			
PRB → PDS	0.276	2.908	0.004	0.276	2.908	0.004			
TT → PDS	-0.173	1.938	0.053	-0.221	2.809	0.005			
TT → PRB	-0.173	1.159	0.247	-0.173	1.159	0.247			
DOC → PRB → PDS							-0.011	0.399	0.690
DOC → TT → PDS							-0.074	1.780	0.075
EA → PRB → PDS							-0.068	1.294	0.196
TT → PRB → PDS							-0.048	1.196	0.232

TABLE 9. Structural estimates (hypothesis testing) for combined demographics.

Structural path	Direct effect			Total effect			Indirect effect		
	Std β	T	P	Std β	T	P	Std β	T	P
DOC → PDS	-0.101	1.737	0.082	-0.170	2.774	0.006			
DOC → PRB	-0.148	2.806	0.005	-0.123	2.268	0.023			
DOC → TT	0.421	9.832	0.000	0.421	9.832	0.000			
EA → DOC	0.441	10.309	0.000	0.441	10.309	0.000			
EA → PDS	0.142	2.385	0.017	-0.061	1.082	0.279			
EA → PRB	-0.332	6.529	0.000	-0.386	8.751	0.000			
EA → TT				0.186	6.267	0.000			
PRB → PDS	0.384	9.549	0.000	0.384	9.549	0.000			
TT → PDS	-0.052	0.721	0.471	-0.029	0.408	0.683			
TT → PRB	0.060	0.989	0.323	0.060	0.989	0.323			
DOC → PRB → PDS							-0.057	2.638	0.008
DOC → TT → PDS							-0.022	0.709	0.479
EA → PRB → PDS							-0.128	5.439	0.000
TT → PRB → PDS							0.023	0.985	0.325

policymakers and AI developers to create adaptable, user-centric privacy regulations that respect ethical norms and guarantee AI systems continue to spur innovation without sacrificing individual autonomy, longitudinal studies are required to monitor changes in user perceptions over time.

F. COLLABORATIVE APPROACHES TO PRIVACY PROTECTIONS

One of the study's main conclusions is how crucial collaboration is to efficient privacy management, especially between parents and young people. The study shows that too restrictive parental engagement can reduce young users'

TABLE 10. Validation of hypotheses.

	Hypothesis	Young Digital Citizens	Parents & Educators	AI Professionals	Combined
H1	DOC has a significant influence on PDS	x	x	√	√
H2	PRB mediates the relationship between DOC and PDS	x	x	x	√
H3	TT has a significant effect on PDS	x	x	√	x
H4	PRB has a direct effect on PDS	x	√	√	√
H5	DOC has a direct effect on PRB	x	x	x	√
H6	EA has a direct effect on PRB	√	x	x	√
H7	PRB has a mediates the relationship between TT and PDS	x	√	x	x
H8	DOC has a direct effect on TT	x	x	√	√
H9	TT has a direct effect on PRB	x	√	x	x
H10	TT mediates the relationship between DOC and PDS	x	x	√	x
H11	EA has a significant influence PDS	x	x	x	√
H12	EA has a total effect on TT	x	x	√	√
H13	EA has a direct effect on DOC	√	√	√	√
H14	PRB mediates the relationship between EA and PDS	x	x	x	√

Notes:√ = True; x = False

TABLE 11. Qualitative questions by demographic group.

Young Digital Citizens	1. What are your main concerns regarding privacy when using AI systems?
	2. What measures do you think should be implemented to enhance privacy in AI systems?
	3. How do you balance the benefits of data usage with the need for privacy protection in your digital activities?
Parents and Educators	1. What are your main concerns regarding privacy in AI systems for young people?
	2. What measures do you think should be implemented to enhance privacy in AI systems for young people?
	3. How do you balance the benefits of data usage with the need for privacy protection for young people in your role as an educator or parent?
AI Researchers and Developers	1. What are your main concerns regarding privacy when using AI systems?
	2. What measures do you think should be implemented to enhance privacy in AI systems?
	3. How do you balance the benefits of data usage with the need for privacy protection in your work?

TABLE 12. Identified risks of personal data use in AI systems by stakeholder group.

	Youth	Parents and Educators	AI Professionals
Loss of Control	Long-term data use by unauthorized parties	Lack of data-sharing education	Unintentional exposure of personal info learned from training data
Surveillance	Facial Recognition and Location Tracking	Online behavior and information tracking	Excessive, non-consensual data collection
Profiling	Informational echo-chambers	Influence over behavior and beliefs	Influence over behavior and beliefs

TABLE 13. Benefits of AI systems by stakeholder group.

	Youth	Parents and Educators	AI Professionals
Educational Advancement	Help with homework	Personalized learning	
Personalized Experiences		Disability and Accessibility	Customized service recommendations
Innovation			Increased workplace reliability and efficiency

TABLE 14. Main privacy concerns in AI systems by stakeholder group.

	Youth	Parents and Educators	AI Professionals
Data Collection Practices	Limited understanding of data-sharing risks	Collection of sensitive information	Risks pertaining to long-term data collection and use
Security and Regulatory Concerns	Long-term and geographic implications for data collection	Data sharing with 3rd party groups	Inadvertent and malicious data exposure
Profiling	Informational echo-chambers	Influence on behavior and beliefs	Influence on behavior and beliefs

autonomy in controlling their privacy by identifying the detrimental effects of excessive parental control on Data Ownership and Control (DOC) in Parental Data Sharing (PDS) ($\beta = -0.170$, p = 0.006). A more balanced, bottom-up strategy that blends teenage empowerment with parental advice is required to get beyond strict, top-down privacy restrictions. To promote shared accountability, privacy education should be co-developed through collaborative talks between young users, educators, parents, and legislators rather than being imposed. Through the provision of resources, interactive learning tools, and industry-led programs that give adults and children the knowledge they need to protect their privacy, collaborative efforts, including public-private partnerships, can aid in closing the digital literacy gaps. Lawmakers must also put in place frameworks that promote moral AI behavior and shared accountability between sectors that handle

TABLE 15. **Privacy measures to enhance privacy in AI systems.**

	Youths	Parents and Educators	AI Professionals
Enhanced Transparency	Platform-level exposure of data use	Explanations of data usage	Accessible Privacy Policies
Data Collection Controls	Accessible privacy controls	Youth and parental privacy controls	Federated learning and differential privacy
Legislation and Regulation	Privacy standards and certifications	Youth-specific regulations	Anonymization and encryption
Education	Institutionalized AI and privacy education	Youth and adult privacy literacy programs	Unspecified 'teaching' of young users

TABLE 16. **Strategies for balancing benefits and privacy protection by stakeholder group.**

	Youths	Parents and Educators	AI Professionals
Selective Data Use	Limit data sharing to essential purposes	Limited sharing of youth data	Developing user-facing controls
Platform Transparency	Evaluation of platform privacy policies	Evaluation of platform privacy policies	Clear communication with users
Privacy Protecting Technology	Privacy-protecting browsers, VPNs, and Ad-blockers		Anonymization, Encryption, and limited storage
Education		Empowering youths to make informed decisions	Inform users through applications

sensitive user data. Future studies should examine how well these cooperative models work in a variety of cultural and demographic contexts and assess how well they encourage appropriate data-sharing practices over time. Such strategies can reduce privacy threats and provide users greater control over their digital identities by encouraging shared accountability, guaranteeing a more moral and user-focused AI environment.

G. STUDY LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

This study offers valuable insights into privacy perceptions within AI-driven environments; however, it also presents several limitations that inform directions for future research. A key limitation relates to the sampling strategy. Data collection focused on three stakeholder groups—young digital citizens, parents and educators, and AI professionals. While these groups provide important perspectives, the exclusion of other relevant stakeholders, such as non-technical users, policymakers, and industry regulators, may limit the broader applicability of the findings. Additionally, the use of convenience sampling introduces the possibility of selection bias, which reduces generalizability. Future research should consider employing probability-based sampling methods across more diverse demographic groups. Another limitation lies in the study's cross-sectional design, which captures privacy attitudes at a single point in time. This approach does not allow for the examination of how perceptions evolve in response to prolonged interactions with AI technologies. Longitudinal studies would provide deeper insight into how privacy concerns and behaviors change over time, especially considering advancing AI capabilities and regulatory developments. While this study engaged multiple stakeholder groups, it did not incorporate formal comparative analysis between them. Future research could explore group-based differences in privacy perceptions and behaviors to uncover more nuanced insights. Moreover, variation in construct reliability across groups suggests that cultural, demographic, or professional differences may influence how individuals interpret privacy-related concepts. Refining measurement instruments to account for these contextual variations will enhance the inclusivity and robustness of future models. Addressing these limitations will support the development of more comprehensive research frameworks and contribute to the evolution of privacy-preserving strategies for responsible AI deployment.

H. IMPLICATIONS FOR POLICY AND ETHICAL AI DEVELOPMENT

The findings of this study offer several implications for future policy and ethical AI development. Ensuring effective privacy management in AI ecosystems requires interdisciplinary collaboration across technical, ethical, and educational domains. Policies and research efforts should be aligned to reflect the dynamic nature of AI technologies and the complexity of privacy-related decision-making. Future research should explore the impact of educational interventions, particularly in underrepresented communities where digital literacy and privacy awareness may vary due to cultural and socioeconomic factors. Longitudinal investigations can further assess the sustained influence of such interventions over time. For policymakers, the results underscore the urgency of developing proactive governance frameworks that emphasize ethical AI development and user-centric design. Transparency mandates should require AI systems to disclose data usage practices, and adaptive consent mechanisms should be integrated into AI design to support real-time, user-controlled privacy settings.

Given the global nature of AI data flows, international collaboration is essential to harmonize privacy regulations and reduce jurisdictional inconsistencies. Cross-border policy alignment will enhance accountability, mitigate risks of data misuse, and promote trust in AI systems. By fostering collaboration between researchers, policymakers, educators, and AI developers, the findings of this study can inform the development of AI systems that balance innovation with strong privacy protections, ultimately contributing to the advancement of ethical and responsible AI governance.

VI. CONCLUSION

This study offers an in-depth examination of how young digital citizens, parents/educators, and AI researchers/developers maneuver through the complex domain of privacy in AI systems, informed by the PCM. The analysis of critical dimensions, including EA, DOC, PRB, TT, and PDS, highlights the diverse dynamics affecting privacy behaviors. EA became a crucial element in enabling people to make informed choices, emphasizing the importance of integrating privacy education into curricula and public awareness campaigns. The significance of transparency and ethical design in building trust and user confidence highlights the pressing need for intuitive, user-centered system interfaces. The interaction of perceived risks and benefits, together with the impact of cooperative strategies among stakeholders, reveals the complex trade-offs involved in privacy management. However, challenges such as varying levels of digital literacy, opaque data practices, and excessive parental intervention remain significant barriers to effective privacy governance. Addressing these challenges requires focused interventions, such as adaptive consent mechanisms, education in risk-benefit analysis, explainable AI tools that clarify how data is used, and inclusive policymaking that reflects the diverse needs of different user groups. Future research should build on these insights by investigating longitudinal trends in privacy perceptions, cross-cultural differences, and the scalability of collaborative frameworks. Such efforts will ensure AI systems remain equitable, ethical, and empowering for all users. This study contributes to the evolution of AI governance by emphasizing education, transparency, and collaboration as foundational pillars for creating a digital ecosystem that balances innovation with robust privacy protections.

ACKNOWLEDGMENT

The views expressed herein are those of the authors and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada (OPC).

REFERENCES

[1] E. Durall Gazulla, N. Hirvonen, S. Sharma, H. Hartikainen, V. Jylhä, N. Iivari, M. Kinnula, and A. Baizhanova, "Youth perspectives on technology ethics: Analysis of teens' ethical reflections on AI in learning activities," *Behav. Inf. Technol.*, vol. 44, no. 5, pp. 1–24, May 2024, doi: 10.1080/0144929x.2024.2350666.

[2] D. D. Choi and P. B. Lowry, "Balancing the commitment to the common good and the protection of personal privacy: Consumer adoption of sustainable, smart connected cars," *Inf. Manage.*, vol. 61, no. 1, Jan. 2024, Art. no. 103876, doi: 10.1016/j.im.2023.103876.

[3] A. K. Shrestha, A. Barthwal, M. Campbell, A. Shouli, S. Syed, S. Joshi, and J. Vassileva, "Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review," in *Proc. IEEE 15th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, 2024.

[4] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, Mar. 2006, doi: 10.1287/isre.1060.0080.

[5] I. Bile Hassan, M. A. A. Murad, I. El-Shekeil, and J. Liu, "Extending the UTAUT2 model with a privacy calculus model to enhance the adoption of a health information application in Malaysia," *Informatics*, vol. 9, no. 2, p. 31, Mar. 2022, doi: 10.3390/informatics9020031.

[6] K. Thai, K. H. Tsiandoulas, E. A. Stephenson, D. Menna-Dack, R. Z. Shaul, J. A. Anderson, A. R. Shinewald, A. Ampofo, and M. D. McCradden, "Perspectives of youths on the ethical use of artificial intelligence in health care research and clinical care," *JAMA Netw. Open*, vol. 6, no. 5, May 2023, Art. no. e2310659, doi: 10.1001/jamanetworkopen.2023.10659.

[7] S. Jia, O. H. Chi, and L. Lu, "Social robot privacy concern (SRPC): Rethinking privacy concerns within the hospitality domain," *Int. J. Hospitality Manage.*, vol. 122, Sep. 2024, Art. no. 103853, doi: 10.1016/j.ijhm.2024.103853.

[8] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," *Comput. Hum. Behav.*, vol. 53, pp. 419–426, Dec. 2015, doi: 10.1016/j.chb.2015.07.025.

[9] C. H. Lee, N. Gobir, A. Gurn, and E. Soep, "In the black mirror: Youth investigations into artificial intelligence," *ACM Trans. Comput. Educ.*, vol. 22, no. 3, pp. 1–25, Sep. 2022, doi: 10.1145/3484495.

[10] Z. Peng, "A privacy calculus model perspective that explains why parents sharent," *Inf., Commun. Soc.*, vol. 27, no. 11, pp. 2129–2152, Aug. 2024, doi: 10.1080/1369118x.2023.2285462.

[11] K. Davis and C. James, "Tweens' conceptions of privacy online: Implications for educators," *Learn., Media Technol.*, vol. 38, no. 1, pp. 4–25, Mar. 2013, doi: 10.1080/17439884.2012.658404.

[12] D. Goyeneche, S. Singaraju, and L. Arango, "Linked by age: A study on social media privacy concerns among younger and older adults," *Ind. Manage. Data Syst.*, vol. 124, no. 2, pp. 640–665, Jan. 2024, doi: 10.1108/imds-07-2023-0462.

[13] S. Youn and W. Shin, "Teens' responses to Facebook newsfeed advertising: The effects of cognitive appraisal and social influence on privacy concerns and coping strategies," *Telematics Informat.*, vol. 38, pp. 30–45, May 2019, doi: 10.1016/j.tele.2019.02.001.

[14] A. Hasse, S. Cortesi, A. Lombana-Bermudez, and U. Gasser, "Youth and artificial intelligence: Where we stand," Berkman Klein Center Internet & Soc., Harvard Univ., May 2019. [Online]. Available: https://cyber.harvard.edu/publication/2019/youth-and-artificial-intelligence/where-we-stand

[15] L. Huang, "Ethics of artificial intelligence in education: Student privacy and data protection," *Sci. Insights Educ. Frontiers*, vol. 16, no. 2, pp. 2577–2587, Jun. 2023, doi: 10.15354/sief.23.re202.

[16] Y. Chen and P. Esmaeilzadeh, "Generative AI in medical practice: In-depth exploration of privacy and security challenges," *J. Med. Internet Res.*, vol. 26, Mar. 2024, Art. no. e53008, doi: 10.2196/53008.

[17] N. Ebert, T. Geppert, J. Strycharz, M. Knieps, M. Hönig, and E. Brucker-Kley, "Creative beyond TikToks: Investigating Adolescents' social privacy management on TikTok," *Proc. Privacy Enhancing Technol.*, vol. 2023, no. 2, pp. 221–235, Apr. 2023, doi: 10.56553/popets-2023-0049.

[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] H. Xu, H.-H. Teo, B. C. Y. Tan, and R. Agarwal, "The role of push-pull technology in privacy calculus: The case of location-based services," *J. Manage. Inf. Syst.*, vol. 26, no. 3, pp. 135–174, Dec. 2009, doi: 10.2753/mis0742-1222260305.

[20] M. Stoilova, R. Nandagiri, and S. Livingstone, "Children's understanding of personal data and privacy online—A systematic evidence mapping," *Inf., Commun. Soc.*, vol. 24, no. 4, pp. 557–575, Mar. 2021, doi: 10.1080/1369118x.2019.1657164.

[21] D. Gunning, M. Stefik, J. Choi, T. Miller, S. Stumpf, and G.-Z. Yang, "XAI—Explainable artificial intelligence," *Sci. Robot.*, vol. 4, no. 37, Dec. 2019, Art. no. eaay7120, doi: 10.1126/scirobotics.aay7120.

[22] G. Singh, A. S. Aiyub, T. Greig, S. Naidu, A. Sewak, and S. Sharma, "Exploring panic buying behavior during the COVID-19 pandemic: A developing country perspective," *Int. J. Emerg. Markets*, vol. 18, no. 7, pp. 1587–1613, Jun. 2023, doi: 10.1108/ijoem-03-2021-0308.

[23] E. Princi and N. C. Krämer, "Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices," *Frontiers Psychol.*, vol. 11, pp. 1–15, Nov. 2020, doi: 10.3389/fpsyg.2020.582054.

[24] 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," *Inf. Syst. J.*, vol. 25, no. 6, pp. 607–635, Nov. 2015, doi: 10.1111/isj.12062.

[25] J. Lou, M. Wang, X. Xie, F. Wang, X. Zhou, J. Lu, and H. Zhu, "The association between family socio-demographic factors, parental mediation and adolescents' digital literacy: A cross-sectional study," *BMC Public Health*, vol. 24, no. 1, p. 2932, Dec. 2024, doi: 10.1186/s12889-024-20284-4.

[26] M. Akter, A. J. Godfrey, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski, "From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?" *Proc. ACM Human-Comput. Interact.*, vol. 6, pp. 1–28, Apr. 2022, doi: 10.1145/3512904.

[27] N. Steinfeld, "Parental mediation of adolescent Internet use: Combining strategies to promote awareness, autonomy and self-regulation in preparing youth for life on the Web," *Educ. Inf. Technol.*, vol. 26, no. 2, pp. 1897–1920, Mar. 2020, doi: 10.1007/s10639-020-10342-w.

[28] N. D. Santer, A. Manago, A. Starks, and S. M. Reich, "Early adolescents' perspectives on digital privacy," in *Algorithmic Rights and Protections for Children*. Cambridge, MA, USA: MIT Press, Jun. 2023, pp. 123–160, doi: 10.7551/MITPRESS/13654.003.0012.

[29] M. C. Buchan, J. Bhawra, and T. R. Katapally, "Navigating the digital world: Development of an evidence-based digital literacy program and assessment tool for youth," *Smart Learn. Environ.*, vol. 11, no. 1, pp. 1–24, Dec. 2024, doi: 10.1186/s40561-024-00293-x.

[30] M. Walrave, S. Robbé, L. Staes, and L. Hallam, "Mindful sharenting: How millennial parents balance between sharing and protecting," *Frontiers Psychol.*, vol. 14, pp. 1–13, Jul. 2023, doi: 10.3389/fpsyg.2023.1171611.

[31] J. Wanner, L.-V. Herm, K. Heinrich, and C. Janiesch, "The effect of transparency and trust on intelligent system acceptance: Evidence from a user-based study," *Electron. Markets*, vol. 32, no. 4, pp. 2079–2102, Oct. 2022, doi: 10.1007/s12525-022-00593-5.

[32] C. Wiencierz and M. Lünich, "Trust in open data applications through transparency," *New Media Soc.*, vol. 24, no. 8, pp. 1751–1770, Aug. 2020, doi: 10.1177/1461444820979708.

[33] *Teen Privacy and Safety Online: Knowledge, Attitudes, and Practices Oakland*. Oakland, CA, USA: Youth Tech Health, 2016. [Online]. Available: https://healtheducationresources.unesco.org/library/documents/teen-privacy-and-safety-online-knowledge-attitudes-and-practices

[34] S. Youn, "Parental influence and Teens' attitude toward online privacy protection," *J. Consum. Affairs*, vol. 42, no. 3, pp. 362–388, Sep. 2008. [Online]. Available: https://portal.issn.org/resource/ISSN/0022-0078

[35] S. Tian, B. Zhang, and H. He, "Role of algorithm awareness in privacy decision-making process: A dual calculus lens," *J. Theor. Appl. Electron. Commerce Res.*, vol. 19, no. 2, pp. 899–920, Apr. 2024, doi: 10.3390/jtaer19020047.

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

[37] M. Jafari and Z. Shaghaghi, "Navigating privacy concerns: Social media users' perspectives on data sharing," *AI Tech. Behav. Social Sci.*, vol. 1, no. 1, pp. 20–26, Jan. 2023, doi: 10.61838/kman.aitech.1.1.4.

[38] P. B. Brandtzaeg, A. Pultier, and G. M. Moen, "Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy," *Social Sci. Comput. Rev.*, vol. 37, no. 4, pp. 466–488, Aug. 2019, doi: 10.1177/0894439318777706.

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

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

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

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

[43] C. E. Koh, V. R. Prybutok, S. D. Ryan, and Y. A. Wu, "A model for mandatory use of software technologies: An integrative approach by applying multiple levels of abstraction of informing science," *Inf. Sci., Int. J. Emerg. Transdiscipline*, vol. 13, pp. 177–203, Jan. 2010, doi: 10.28945/1326.

[44] 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.

[45] 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.

[46] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training," *MIS Quart.*, vol. 34, no. 4, pp. 757–778, Dec. 2010, doi: 10.5555/2017496.2017502.

[47] 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," *J. Amer. Soc. for Inf. Sci. Technol.*, vol. 58, no. 2, pp. 157–165, Jan. 2007, doi: 10.1002/asi.20459.

[48] 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 *Proc. IEEE 4th Int. Conf. AI Cybersecur. (ICAIC)*, Feb. 2025, pp. 1–10, doi: 10.1109/ICAIC63015.2025.10848639.

[49] M. Campbell, A. Barthwal, S. Joshi, A. Shouli, and A. K. Shrestha, "Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis," in *Proc. IEEE 15th Annu. Comput. Commun. Workshop Conf. (CCWC)*. USA: IEEE, Jan. 2025, pp. 00030–00037.

[50] A. K. Shrestha and J. Vassileva, "User acceptance of usable blockchain-based research data sharing system: An extended TAM-based study," in *Proc. 1st IEEE Int. Conf. Trust*, Dec. 2019, pp. 203–208, doi: 10.1109/TPS-ISA48467.2019.00033.

[51] W. W. Chin, B. L. Marcolin, 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," *Inf. Syst. Res.*, vol. 14, no. 2, pp. 189–217, Jun. 2003, doi: 10.1287/isre.14.2.189.16018.

[52] 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, p. e502, May 2021, doi: 10.7717/peerj-cs.502.

[53] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed. Thousand Oaks, CA, USA: SAGE Publications, 2017.

[54] W. W. Chin, R. A. Peterson, and S. P. Brown, "Structural equation modeling in marketing: Some practical reminders," *J. Marketing Theory Pract.*, vol. 16, no. 4, pp. 287–298, Sep. 2008, doi: 10.2753/mtp1069-6679160402.

[55] J. F. Hair Jr., M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research," *Eur. Bus. Rev.*, vol. 26, no. 2, pp. 106–121, Mar. 2014, doi: 10.1108/ebr-10-2013-0128.

[56] G. Demo, E. R. Neiva, I. Nunes, and K. Rozzett, "Human resources management policies and practices scale (HRMPPS): Exploratory and confirmatory factor analysis," *BAR - Brazilian Admin. Rev.*, vol. 9, no. 4, pp. 395–420, Sep. 2012, doi: 10.1590/s1807-76922012005000006.

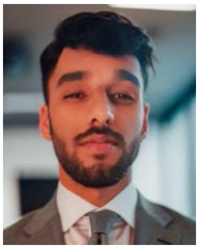
[57] P. R. Warshaw and F. D. Davis, "Disentangling behavioral intention and behavioral expectation," *J. Experim. Social Psychol.*, vol. 21, no. 3, pp. 213–228, May 1985, doi: 10.1016/0022-1031(85)90017-4.

[58] A. K. Shrestha and S. Joshi, "Toward ethical AI: A qualitative analysis of stakeholder perspectives," in *Proc. IEEE 15th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2025, pp. 22–29, doi: 10.1109/CCWC62904.2025.10903879.

AUSTIN SHOULI was born in Kitchener, Waterloo, ON, Canada, in 1995. He received the Diploma degree in journalism from the Southern Alberta Institute of Technology, Calgary, AB, Canada, in 2019. He is currently pursuing the B.Sc. degree in computer science with Vancouver Island University, Nanaimo, BC, Canada.

He is also a Research Assistant with Vancouver Island University, working with a team funded by the Office of the Privacy Commissioner of Canada, under the supervision of Prof. Ajay Shrestha, studying questions of privacy as they pertain to young digital citizens and artificial intelligence. He plans to continue research in artificial intelligence by pursuing a graduate degree in computer science.

Mr. Shouli was a recipient of the Best Paper Award in the data mining category at 2024 IEEE IEMCON Conference.



ANKUR BARTHWAL was born in Dehradun, India. He received the B.B.A. degree from the University of Petroleum and Energy Studies, India, in 2018, and the M.B.A. degree from Vancouver Island University, Nanaimo, BC, Canada.

He was a Business Development Executive, from 2019 to 2022. He has been a Project Personnel with Vancouver Island University, since 2024, where he participates in the Office of the Privacy Commissioner of Canada-funded research on teenage privacy problems in AI systems, under the supervision of Prof. Ajay Shrestha. He has authored several research papers at IEEE conferences.

Mr. Barthwal was a recipient of the Best Paper Award in the data mining category at 2024 IEEE IEMCON.

MOLLY CAMPBELL was born in Newmarket, ON, Canada, in 1995. She received the B.M. degree in statistics from Carleton University, in 2017. She is currently pursuing the B.S. degree in computer science with Vancouver Island University.

She is also a Research Assistant with Vancouver Island University, working with a team funded by the Office of the Privacy Commissioner of Canada, under the supervision of Prof. Ajay Shrestha, where she is part of a project ‘‘Investigating Youth's Perspective on Privacy Within AI Systems.’’ Her team has published several papers within the scope of this research.

Mrs. Campbell was a recipient of the Best Paper Award in the data mining category at 2024 IEEE IEMCON.

AJAY KUMAR SHRESTHA (Member, IEEE) received the M.Sc. degree in ethical hacking and computer security from the University of Abertay Dundee, Scotland, U.K., in 2013, and the Ph.D. degree in computer science from the University of Saskatchewan, Canada, in 2022. His Ph.D. research leveraged blockchain and smart contract technologies to facilitate data sharing with user-controlled privacy, establishing guidelines that embed privacy, user control, and incentives into data-sharing frameworks.

He is currently a Professor with Vancouver Island University, BC, Canada, and an Adjunct Professor with the University of Saskatchewan. He was a Cybersecurity Specialist and has contributed to industry-led research on privacy-conscious and blockchain-based data-sharing frameworks. He has authored several award-winning papers presented at IEEE conferences and published in high-impact journals. He is involved as the Principal Investigator with an Office of the Privacy Commissioner of Canada (OPC)-funded project examining youth privacy in AI systems. His research focuses on blockchain, data trust, privacy-preserving technologies, and ethical AI.

Dr. Shrestha holds a lifetime membership with the Services Society (S2). He has served on the technical program committees for various IEEE and ACM conferences and has received multiple accolades, including the best paper and best presentation awards at IEEE events. He was recognized as a Young Innovator by The StarPhoenix; and received the Dean's Scholarship and the Teacher-Scholar Doctoral Fellowship during the doctoral studies and the Erasmus Mundus Scholarship for the master's program.