Applying Communication Privacy Management Theory to Youth Privacy Management in AI Contexts

Molly Campbell
Computer Science Department
Vancouver Island University
Nanaimo, Canada
molly.campbell@viu.ca

Sandhya Joshi
VIU Affiliate
Vancouver Island University
Nanaimo, Canada
sandhya.joshi@viu.ca

Ankur Barthwal
Computer Science Department
Vancouver Island University
Nanaimo, Canada
ankur.barthwal@viu.ca

Austin Shouli
Computer Science Department
Vancouver Island University
Nanaimo, Canada
austin.shouli@viu.ca

Ajay Kumar Shrestha
Computer Science Department
Vancouver Island University
Nanaimo, Canada
ajay.shrestha@viu.ca

2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC) | 979-8-3315-1888-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICAIC63015.2025.10848639

***Abstract*— The rapid integration of Artificial Intelligence (AI) technologies into the lives of young digital citizens has escalated privacy concerns and the need for critical examination. This study uses Communication Privacy Management (CPM) Theory to understand how youth and critical stakeholders navigate these concerns. A total of 306 participants were surveyed, comprising 146 AI professionals, 127 parents and educators and 33 youths (aged 16-19). Employing a mixed-methods approach, the research combined quantitative data from structured questionnaires with qualitative insights from open-ended responses. Descriptive statistics reveal distinct perspectives among different demographics regarding data ownership, education, transparency and trust, parental role and perceived risks and benefits associated with AI systems. Structural equation modelling identified key influences on youth privacy management, highlighting the significance of transparency and trust, education and awareness, and parental data sharing among AI professionals, parents, educators, and young digital citizens. The qualitative analysis further underscored unique concerns, emphasizing a lack of understanding and data misuse contributed to the feeling of helplessness shared by all stakeholders. This study underscores the importance of integrating diverse stakeholders' perspectives in the development of AI systems to address the complex challenges faced by youth. Recommendations include collaborative policymaking, implementing user-centric design practices, and enhancing privacy education to empower young digital citizens.**

Keywords*— *Privacy, Artificial Intelligence, Youth, Generative AI, Communication Privacy Management Theory, User control, Data Ownership, Parental Data Sharing, Transparency, Trust, Education, Awareness

I. Introduction

The evolution of Artificial Intelligence (AI) technologies has profoundly reshaped daily life, particularly for young digital citizens who are often at the forefront of adopting innovations [1], [2]. AI-driven systems ranging from virtual assistants to social media algorithms and personalized learning platforms rely heavily on extensive data collection to provide personalized experiences and improved services. These technologies undoubtedly have benefits, but they also pose serious problems concerning data ownership, privacy, and ethical use of personal data [1].

Young digital citizens [2] are commonly defined as digital natives growing up in a digital era where sharing personal information online over social media has become normalized. Many in this demographic have limited awareness of the complexities of data privacy and the potential long-term risks of their information disclosures. This lack of understanding leaves them particularly vulnerable to privacy breaches, identity theft and the misuse of their data. Compounding this issue, the lack of transparency and technical complexity of AI systems often hinder young users from making informed choices regarding their privacy. Even though AI is omnipresent in young digital citizens' lives, research exploring how they handle privacy issues within AI-driven environments is limited [3]. The current state of the art tends to concentrate mainly on adult populations or broad privacy issues, ignoring the difficulties that young digital citizens encounter when engaging with AI-driven platforms. This emphasizes the necessity of looking into the variables affecting how youth handle their privacy to improve policy frameworks, educational initiatives, and AI design methodologies.

To address this knowledge gap, this study uses the Communication Privacy Management (CPM) Theory [4] as a framework for understanding youth privacy management behaviors in AI contexts. CPM Theory emphasizes how individuals regulate the disclosure of personal information through key processes, including privacy ownership, control, rulemaking, and the management of boundary turbulence that occurs when privacy expectations are violated. This study specifically examines five variables: Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA) [2]. Together, these constructs provide a comprehensive view of the interactions between individual perceptions, parental roles, system transparency, and educational factors in shaping privacy management behaviors. While CPM Theory has been applied in other contexts, its relevance to youth privacy management within AI environments has not yet been fully explored.

In this study, we gathered survey data from 306 participants, including 146 AI developers and researchers, 127 parents and educators, and 33 young digital citizens between the ages of 16

The Office of the Privacy Commissioner of Canada's Contributions Program.

and 19. The hypotheses produced from CPM Theory were tested and the interactions between the constructs were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) technique. This work intends to close a significant gap in the literature and offer practical suggestions for improving youth privacy management in AI contexts by fusing CPM Theory with empirical data. In addition to broadening the theoretical applicability of CPM Theory to contemporary technological contexts, this research provides insightful information for AI developers, educators, and policymakers.

The rest of the paper is organized as follows: the next section provides an overview of related works and background literature. The methodologies are outlined in section III. Section IV presents the results of our study. Section V provides the discussion with recommendations for ethical AI practices, limitations, and future research direction. Finally, Section VI concludes the paper.

II. Background and Related Works

A. Communication Privacy Management Theory

Developed by Sandra Petronio [4], Communication Privacy Management (CPM) Theory serves as a foundational framework for understanding how individuals make decisions about sharing or withholding private information. CPM emphasizes that people view private information as their possession, granting them the autonomy to control and regulate its disclosure based on personal privacy rules. These privacy rules are shaped by various factors, including cultural norms, motivations, assessments of risks and benefits, and contextual circumstances [4].

The theory outlines some fundamental key principles that are particularly relevant to comprehending how to maintain young digital citizens' privacy in AI-driven environments:

1) Privacy Ownership: People think they own their private information and are entitled to control how it is disclosed.

2) Privacy Control: Techniques are used to manage the accessibility and flow of personal data.

3) Privacy Rules: Established guidelines that take into account a variety of influencing elements serve as a reference for personal privacy decisions.

4) Privacy Boundaries: Symbolic boundaries that assist people regulate what they share by separating private information from public information.

5) Boundary Coordination: When private information is shared with others, there is a process of negotiation to manage shared privacy boundaries.

6) Boundary Turbulence: When privacy norms are broken, there are disturbances that result in disagreements or the need to renegotiate privacy boundaries.

B. Constructs Being Examined

Table I provides the definitions of the five key constructs examined in our study: Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA).

TABLE I. Constructs And Definition

Construct	Definition
Data Ownership and Control (DOC) [19], [20], [21], [22]	It is the degree to which young people have control over their personal data and engage in discussions about privacy.
Parental Data Sharing (PDS) [23], [24], [25]	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)[22], [24], [26]	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) [27], [28], [29]	It is the degree to which transparency in data usage influences trust in AI systems.
Education and Awareness (EA) [30], [31], [32], [33]	It is the degree to which stakeholders are informed about privacy and ethical issues associated with AI.

In an era where AI systems increasingly collect and analyze personal information, youths' sense of ownership is often challenged by the opaque and complex nature of data practices [5], [6]. A strong sense of ownership is linked to privacy-protective behaviors, empowering young individuals to establish boundaries and exercise autonomy over their data [1]. However, the intricacy of AI systems and the lack of user-friendly privacy controls frequently undermine their ability to maintain such control [7]. Studies reveal that youths often have a limited understanding of data ownership, which further hampers their ability to effectively manage their privacy in AI-driven environments [8].

As parental involvement can be instrumental in guiding and educating children about privacy risks, it also has the potential to inadvertently undermine youths' privacy management through the over-disclosure of personal information [9]. Striking a balance between parental authority and youths' autonomy requires careful boundary coordination to ensure that privacy rights are respected. Open and effective communication between parents and their children fosters the negotiation of privacy boundaries, thereby minimizing the likelihood of boundary turbulence and associated conflicts [10].

Furthermore, PRB plays a critical role in shaping how youth decide whether to disclose personal information to AI systems. According to CPM Theory, individuals weigh the potential benefits against the associated risks before making decisions about sharing private information [11]. For youth, the perceived advantages, such as personalized content and improved user experiences, often outweigh the concerns of risks like data breaches or misuse, prompting them to share their data more readily [12]. However, understanding how young digital citizens assess these risks and benefits is vital to developing effective strategies that support their privacy management. Studies reveal that young individuals tend to perceive risks at a lower level than adults, which can result in more permissive data-sharing behaviors [13].

Additionally, TT is pivotal in influencing how youth approach privacy management in AI systems. Transparent AI technologies that clearly communicate data collection and usage practices foster greater trust, encouraging users to share personal information with confidence [14]. Trust acts as a critical factor in shaping how individuals set and negotiate

privacy boundaries, determining their willingness to disclose information. Conversely, a lack of transparency can erode trust, making users hesitant to engage or share data. Enhancing transparency in AI systems not only mitigates perceived risks but also establishes a foundation for stronger, more trusting relationships between youth and technology [15].

EA also plays a critical role in equipping youth with the tools needed for effective privacy management. Within the framework of CPM, knowledge and understanding of privacy issues are essential for developing informed privacy rules and making deliberate decisions about sharing personal information [16]. Educational initiatives that focus on increasing awareness about AI technologies, data handling practices, and privacy rights empower youth to assert greater control over their personal information, reducing their susceptibility to privacy violations [17]. Research highlights that higher levels of digital literacy are associated with more cautious and thoughtful online behavior among youth, reinforcing the importance of education in promoting responsible digital engagement [18].

C. *Application of CPM to Youth Privacy in AI Contexts*

Applying CPM Theory to youth privacy management in AI environments involves a comprehensive integration of personal, social, and technological dimensions. This theoretical framework offers insights into how young individuals navigate privacy by examining key factors such as control over their data, parental control, risk and benefit assessments, transparency in AI systems, and awareness. Despite its significant applicability, prior research has predominantly addressed privacy concerns among adult populations within general contexts, leaving a gap in understanding the specific experiences and challenges faced by youth in AI-driven interactions [8]. This study bridges that gap by employing CPM to analyze empirical data, shedding light on the unique privacy behaviors of young digital citizens and providing valuable contributions to both theoretical discourse and actionable policy design.

III. Methodology

A. *Research Goal and Questions*

Our research's main goal was to apply CPM Theory to comprehend how young digital citizens maintain their privacy with regard to AI technologies by examining the relationships among five validated constructs: DOC, PDS, PRB, TT, and EA. We aimed to address the following research questions, which serve as the basis for the conceptual framework illustrated in Fig. 1:

- **RQ1:** How do youth develop privacy rules regarding their personal data when interacting with AI technologies?
- **RQ2:** What role do parents play in shaping youths' privacy boundaries and data-sharing behaviors?
- **RQ3:** How do perceived risks and benefits influence youths' decisions to disclose personal information to AI systems?

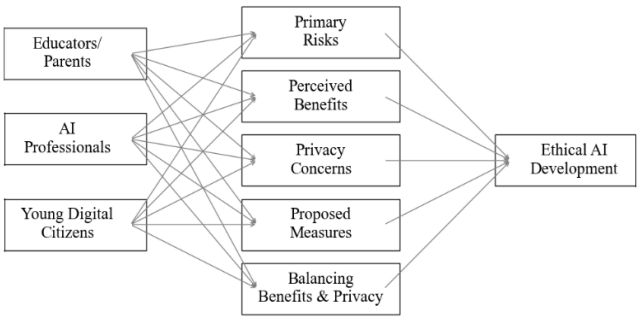

Fig. 1. Stakeholder perspectives leading to ethical AI development

- **RQ4:** In what ways do transparency and trust in AI systems affect youths' privacy management?
- **RQ5:** How do education and awareness about AI and data privacy impact youths' control 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 I, which details their scope and focus within the study.

B. *Research Model and Hypotheses:*

Based on the findings from the literature review, we have developed thirteen research hypotheses aligned with different research questions to examine the constructs detailed in Table I.

The hypotheses associated with RQ1 are outlined below:

- H1: Education and Awareness (EA) positively influences Data Ownership and Control (DOC).
- H2: Perceived Risks and Benefits (PRB) positively influences Data Ownership and Control (DOC).
- H3: Transparency and Trust (TT) positively influences Data Ownership and Control (DOC).
- H4: Perceived Risks and Benefits (PRB) mediates the relationship between Education and Awareness (EA) and Data Ownership and Control (DOC).
- H5: Perceived Risks and Benefits (PRB) mediates the relationship between Transparency and Trust (TT) and Data Ownership and Control (DOC).

The hypotheses associated with RQ2 are outlined below:

- H6: Parental Data Sharing (PDS) positively influences Data Ownership and Control (DOC).
- H7: Parental Data Sharing (PDS) positively influences Education and Awareness (EA).
- H8: Education and Awareness (EA) mediates the relationship between Parental Data Sharing (PDS) and Data Ownership and Control (DOC).

The hypotheses associated with RQ3 are outlined below:

- H9: Perceived Risks and Benefits (PRB) positively influences youths' Privacy Disclosure Decisions (PDD). Note: While PDD is not explicitly listed as a construct, it can be considered an outcome variable related to DOC.

The hypotheses associated with RQ4 are outlined below:

- H10: Transparency and Trust (TT) positively influences Perceived Risks and Benefits (PRB).
- H11: Transparency and Trust (TT) has an indirect effect on Data Ownership and Control (DOC) through Perceived Risks and Benefits (PRB).

The hypotheses associated with RQ5 are outlined below:

- H12: Education and Awareness (EA) positively influences Perceived Risks and Benefits (PRB).
- H13: Education and Awareness (EA) has both a direct and indirect effect on Data Ownership and Control (DOC) through Perceived Risks and Benefits (PRB).

C. Research Design

The present study received ethics approval from the Vancouver Island University Research Ethics Board (VIU-REB). The approval with reference number #103116 was given for behavioral application/amendment forms, consent forms and questionnaires. We conducted a pilot study with six participants, including members of empirical research specialists from the University of Saskatchewan and Vancouver Island University. The pilot study aimed to assess the feasibility and duration of the research approach and refine the study design. Participants provided general feedback on the questionnaire which informed modifications and restructuring of the final survey questionnaires. The revised research model was then assessed by gathering survey data. We recruited participants through flyers, emails, personal networks, and on social networking sites, LinkedIn, and Reddit. To reach young digital citizens, we spoke with several school districts for their assistance in distributing our survey to their high-school students. Participation was entirely voluntary and did not receive any form of compensation. The participants had to read and accept a consent form to participate in the study, by submitting the consent form before starting the questionnaire participants were indicating they understood the conditions of participation in the study outlined in the consent form. We conducted online surveys through Microsoft Forms by requesting each participant to respond to the questionnaire based on our three designated demographics: AI Researchers and Developers, Teachers and Parents, and Youth aged 16-19.

The survey instruments are adapted from constructs validated in prior studies [19], [20], [21], [22], [23], [24], [25], [22], [24], [26], [27], [28], [29], [30], [31], [32], [33]. The instrument consists of 3 indicators for Data Ownership and control (DOC), 2 indicators for Parental Data Sharing (PDS), 4 indicators for Perceived Risk and Benefit (PRB), 3 indicators for Trust and Transparency (TT), 3 indicators for Education and Awareness (EA), and 3 open-ended discussion questions. The respective items (questions) within these constructs are detailed in Table II.

TABLE II. 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. Qpen-Ended Question: Primary risks associated with personal data use. Qpen-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.

We measured responses to the items, excluding qualitative items, on a 5-scale Likert scale. Notably, to ensure consistency in outcomes, we reversed the scale for items in PRB for AI Researchers and Developers and swapped items 1 and 2 in PDS for Young Digital Citizens to align contextually with the items in PRB and PDS for the other demographics. The open-ended questions and 2 indicators from PRB were used for qualitative analysis, while the remaining items were used for quantitative analysis.

D. Participants demographics

A total of 326 participants took part in the study: 132 were parents and/or educators, 153 were AI professionals, and 41 were young digital citizens (aged 16–19). After data cleaning, 127 valid responses from educators/parents, 146 valid responses from AI professionals, and 33 valid responses from young digital citizens remained for analysis. Of the 127 valid educator and/or parent responses, 54 identified as parents, 46 as educators, and 27 identified as both. Among the 146 valid responses from AI professionals, 46 identified AI developers, 98 as AI researchers, and 2 as both. Table III highlights the characteristics of the demographics of the participants.

TABLE III. PARTICIPANTS' DEMOGRAPHICS

Respondents' characteristics	Percentage
Parents	43%
Educators	36 %
Both Parent and Educator	21%
AI Developers	32%
AI Researchers	67%
Both AI Researcher and Developer	1%

IV. Results

This study expands our previous research [34] by focusing specifically on young digital citizens, exploring their unique perspectives on privacy in AI systems alongside the insights gathered from parents/educators and AI professionals. This approach allows us to delve deeper into the privacy concerns and awareness levels of the younger demographic, highlighting their specific challenges and needs in the context of AI.

For data processing, Microsoft Excel was employed to manage the collected data through descriptive statistics. We consolidated data from various demographic groups—including educators, parents, AI professionals, and young digital citizens—into a single dataset for streamlined analysis. The analysis was conducted using a partial least squares structural equation modeling (PLS-SEM) approach via smartPLS software [35]. PLS-SEM is a robust method commonly used to estimate path coefficients in structural models, widely recognized in numerous studies [36], [37]. The SEM as suggested by [38] includes the testing of measurement models (exploratory factor analysis, internal consistency, convergent validity, Dillon-Goldstein's rho) and the structural model (regression analysis). We employed the path-weighing structural model scheme in smartPLS which provides the highest R^2 values for dependent latent variables.

Additionally, a nonparametric bootstrapping procedure was utilized to assess the statistical significance of the PLS-SEM results. Bootstrapping is a resampling technique that creates an empirical sampling distribution by drawing repeated samples with replacements from the original data set. For our analysis, 5,000 subsamples were generated, and a two-tailed test was conducted at a significance level of 0.1.

We also conducted a thematic analysis of open-ended questions to identify common themes expressed by participants.

A. Descriptive Statistics

Our quantitative survey used a 5-point Likert scale to compare mean responses across five key constructs, as shown in Fig. 2. Parents/educators and AI developers/researchers had similar mean scores, while young digital citizens reported lower means, indicating a gap in perceptions. Data Ownership and Control (DOC) was prioritized by all groups: parents/educators scored 3.75, researchers/developers 3.95, and youth 3.32, highlighting the importance of user autonomy over personal data.

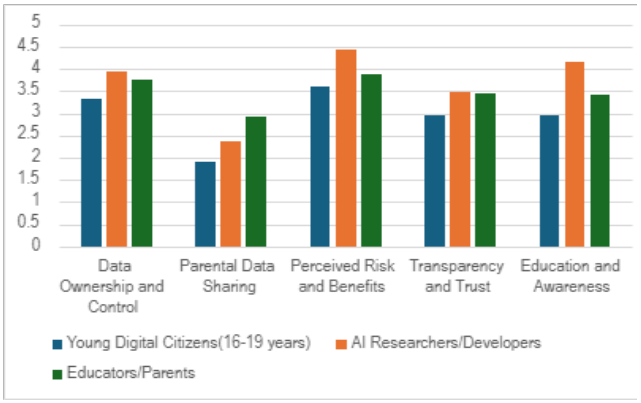

Fig. 2. Analysis of all Constructs

For Transparency and Trust (TT), parents/educators averaged 3.46 and researchers/developers 3.49, while youth scored lower at 2.95, suggesting less trust in AI systems. Parental Data Sharing (PDS) received low scores across groups: 2.94 for parents/educators, 2.36 for researchers/developers, and 1.91 for youth indicating reluctance towards data-sharing behaviors, especially among AI professionals who rated it lower than parents/educators. Perceived Risks and Benefits (PRB) had the highest ratings: parents/educators 3.88, researchers/developers 4.43, and youth 3.61, showing recognition of the ethical implications of AI data practices. Researchers/developers emphasized this aspect more, reflecting their awareness of the broader impacts. Education and Awareness (EA) revealed the largest gap: parents/educators rated it at 3.43, researchers/developers at 4.16, and youth at 2.94. This suggests adults value knowledge of AI and privacy, while youth may lack awareness of its importance.

Overall, while adults agree on user control, transparency, and engagement with AI, youth show lower trust and awareness, highlighting the need for targeted interventions to bridge this gap.

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 loadings of individual items shown in Table IV, to see how each variable loaded on its own construct over the other respective constructs. Factor loadings greater than 0.60 can be considered as significant according to [39]. In our study, all the indicators in the measurement model had a factor loading of value greater than 0.60 except for item 2 in the contrust Trust and Transparency (TT), and item 1 in the Data Ownership and Control (DOC) construct. Item tt2 had a low loading value of 0.344 which would suggest that it be avoided in the model. Although we did use the validated constructs, our exploratory analysis showed that tt2 had a weak influence on Trust and Transparency. Item doc1 had a factor loading value of 0.536, which is just under the significant level of 0.60, which is still deemed moderately acceptable [39].

2) Construct reliability and validity: We assessed convergent validity for each construct by calculating Average Variance Extracted (AVE) and Composite Reliability (CR) from factor loadings (see Table V). AVE should exceed 0.50, indicating that 50% of the variance in the items is captured by the hypothesized constructs, and CR should be above 0.75 [40]. In our study, AVE exceeded 0.50 for all constructs except for Trust and Transparency (TT) and Data Ownership and Control (DOC), which also had CR values slightly below 0.75. TT, with an AVE of 0.449 and CR of 0.686, suggests that it did not capture significant variance to converge into a single construct.

TABLE IV. EXPLORATORY FACTOR ANALYSIS

Construct	Item	Factor Loading
DOC	doc1	0.536
	doc2	0.775
	doc3	0.759
PDS	pds1	0.674
	pds2	0.986
PRB	prb1	0.689
	prb2	0.795
TT	tt1	0.684
	tt2	0.344
	tt3	0.872
EA	ea1	0.840
	ea2	0.609
	ea3	0.760

DOC had a moderate AVE of 0.488 and a CR of 0.736, suggesting marginal acceptability. For Perceived Risks and Benefits (PRB), while the CR was slightly low at 0.711, the acceptable AVE of 0.553 indicates reasonable internal consistency. The other constructs showed CR values over 0.75.

Table V also presents rho_A values (Dillon-Goldstein's rho), which assess within-scale consistency and are preferred over Cronbach's alpha in SEM [41]. DOC achieved a rho_A of 0.510, suggesting moderate reliability. EA scored 0.622, also reflecting moderate reliability. PDS scored 2.062, which is above the acceptable range. This indicates significant variation within the response items, most likely due to the combination of all three demographics, students, parents/educators, and AI developers/researchers, who may have differing opinions. In contrast, PRB exhibited a low score of 0.197, suggesting poor reliability and questioning its appropriateness for inclusion in further analysis. Finally, TT achieved a rho_A of 0.529, indicating moderate reliability.

Overall, while most constructs exhibited acceptable levels of reliability, the PRB and PDS constructs may require reconsideration in future analyses due to their scores.

C. Structural Models

The results of our PLS-SEM analysis [42] are depicted in Fig. 3, featuring coefficients of determination (R^2's), path coefficients (β), and p-values. The R^2 values indicate the variance explained in each construct by its antecedents, while the β values measure the strength of relationships between constructs. P-values assess the statistical significance of these relationships. According to Chin's guideline [24], [43], a β should be at least 0.2 to be considered relevant. Following guidelines from [24], [43], 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. Table VI presents the standardized path coefficients (β), t-statistics, and p-values for the model.

TABLE V. CONSTRUCT RELIABILITY AND VALIDITY

Construct	rho_A	AVE	CR
DOC	0.510	0.488	0.736
PDS	2.062	0.713	0.828
PRB	0.197	0.553	0.711
TT	0.529	0.449	0.686
EA	0.622	0.551	0.784

Fig. 3 in our analysis presents a structural model illustrating the causal relationships among Data Ownership and Control (DOC), Trust and Transparency (TT), Education and Awareness (EA), Perceived Risk and Benefit (PRB), and Parental Data Sharing (PDS). The model explores both direct and indirect effects among these constructs.

Direct effects analysis showed that EA significantly and positively affects DOC ($\beta = 0.329$; $p < 0.001$) and PRB ($\beta = 0.524$; $p < 0.001$), supporting hypotheses H1 and H12. In contrast, PDS exhibits a significant negative impact on DOC ($\beta = -0.170$; $p < 0.01$), leading us to partially reject H6 as the effect, though significant, is negative. TT also shows a positive influence on DOC ($\beta = 0.300$; $p < 0.001$) and a moderately positive effect on PRB ($\beta = 0.300$; $p < 0.1$), affirming hypotheses H3 and H10. However, the relationships between PRB and DOC ($\beta = 0.037$; $p > 0.1$) and between PDS and EA ($\beta = -0.034$; $p > 0.1$) did not reach significance, resulting in the rejection of hypotheses H2, H7, and H9.

The explanatory power of the model is noteworthy, with EA, TT, PDS, and PRB explaining 32.2% of the variance in DOC ($R^2 = 0.322$), and EA and TT explaining 33.4% of the variance in PRB ($R^2 = 0.334$). PDS, however, accounts for only a minimal 0.1% of the variance in EA ($R^2 = 0.001$).

Examining the indirect effects, the analysis indicated that the pathway from PDS to DOC via EA was not significant ($\beta = -0.011$; $p > 0.1$), leading to the rejection of hypothesis H8. Similarly, the indirect pathway from EA to DOC via PRB was insignificant ($\beta = 0.020$; $p > 0.1$), resulting in the rejection of hypothesis H4. Furthermore, the mediation from TT to DOC through PRB was also not supported ($\beta = 0.005$; $p > 0.1$), rejecting hypotheses H5 and H11. Despite EA's direct impact on DOC, its indirect influence through PRB is unsupported, leading to the rejection of hypothesis H13.

These findings elucidate the complex interplay between educational awareness, trust, perceived risks, and parental influences in shaping data ownership and control among youth. Future research should expand on these findings with longitudinal data to better understand the dynamic changes and causal relationships over time.

D. Qualitative findings

Building upon our previous research detailed in [44], this study extends the qualitative analysis of stakeholder perspectives on privacy in AI systems. We further explored the viewpoints of educators, parents, AI professionals, and young digital citizens, examining open-ended survey responses to identify common themes around privacy concerns, which include lack of awareness, data misuse, and feelings of loss of control.

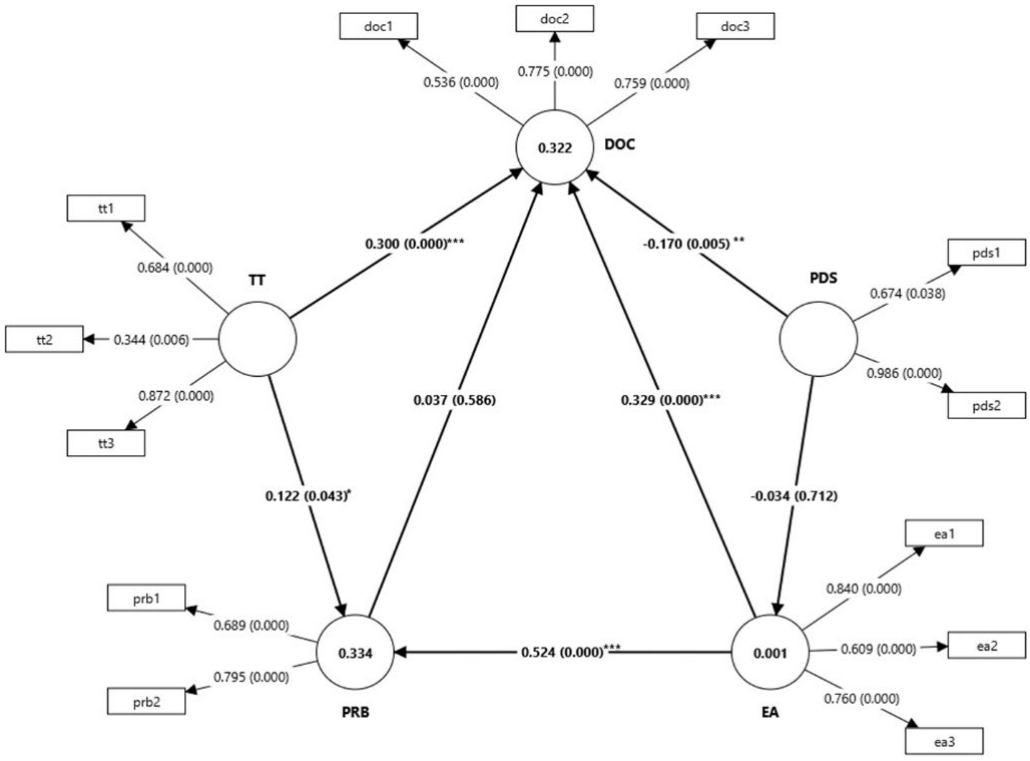

Fig. 3. Structural model showing test results (direct). *p < 0.1; **p < 0.01; ***p < 0.001

TABLE VI. SEM ANALYSIS

Structural path	Std β	T	P
EA → DOC	0.329	5.448	0.000
EA → PRB	0.524	9.979	0.000
PDS → DOC	-0.170	2.810	0.005
PDS → EA	-0.034	0.369	0.712
PRB → DOC	0.037	0.545	0.586
TT → DOC	0.300	5.253	0.000
TT → PRB	0.122	2.023	0.043
PDS → EA → DOC	-0.011	0.350	0.726
TT → PRB → DOC	0.005	0.433	0.665
EA → PRB → DOC	0.020	0.546	0.585

In line with the prior findings [44], Young digital citizens repeatedly expressed a limited understanding of AI data practices, highlighting significant gaps in their knowledge and awareness. For example, one young participant remarked, "I do not know enough about them to be concerned about what I should be concerned about" (#Participant 1). This feeling was shared by parents and educators who expressed concern about the potential dangers of uninformed data sharing in regards to children's safety. A concerned parent noted, "Unauthorized access to personal data can harm children in ways they don't even understand yet" (#Participant 2).

The misuse of data was a critical concern shared by all participants who expressed worry about how their information might be exploited. A youth participant expressed unease about corporate misuse of data, stating, "What worries me is the companies involved misusing, selling, and storing my data for purposes other than personalizing" (#Participant 3). An AI researcher pointed out a systemic liability, adding, "Once data is shared, there's no going back. Misuse becomes inevitable" (#Participant 4).

All three demographics expressed the feeling of powerlessness over the control of personal information being used by AI systems. One educator criticized the excessive demand for data, stating, "AI systems ask for too much data, more than they need to serve their purpose" (#Participant 5). Echoing this concern, a young participant reflected: "AI collects too much personal stuff. Most of us don't know what they do with the data, which feels like losing control" (#Participant 6).

These findings emphasize the challenges associated with the CPM framework concepts of boundary turbulence and privacy control. The responses highlight an urgent need for increased transparency, trust, and education to empower all stakeholders to manage their privacy more effectively in AI environments.

V. DISCUSSION

A. *Education and Awareness Enhances Data Control and Risk Perception*

Education and Awareness (EA) was a significant factor in enhancing the perception of Data Ownership and Control

(DOC). Higher levels of awareness were associated with greater confidence in managing personal data, supported by the construct's reliability metrics (AVE = 0.553, CR = 0.711). These findings align with the principle that knowledge is fundamental in establishing privacy boundaries. Educating individuals about privacy issues gives them the tools to establish strong privacy guidelines, allowing them to manage risks and benefits more effectively. However, the absence of significant mediating effects through Perceived Risks and Benefits (PRB) suggests that theoretical understanding alone may not lead to effective privacy management. Practical training, such as workshops and interactive exercises, may help close the gap by empowering individuals to apply their knowledge in real-life situations.

B. Parental Data Sharing (PDS) Facilitates Privacy Management

Parental Data Sharing (PDS) had a meaningful impact on youth's privacy management, with the study finding a significant yet negative effect on DOC ($\beta = -0.170$, $p = 0.005$). This suggests that overly controlling parental behavior might be undermining youth's confidence in managing their privacy. Collaboration over boundary management control, where parents guide instead of dictate, proves to be more effective in fostering healthy data-sharing practices. Interestingly, PDS did not significantly affect Education and Awareness (EA), highlighting the need for more structured family-oriented educational programs. These types of initiatives should focus on promoting mutual respect and understanding in data-sharing practices in order to reduce boundary turbulence and foster a more balanced dynamic between parents and youth.

C. Perceived Risks and Benefits (PRB) Shape Decisions

Perceived Risks and Benefits (PRB) significantly influenced DOC, with youths who recognized potential risks associated with AI systems exerting more control over their personal data. This underscores the importance of risk awareness in influencing privacy behaviors, highlighted by individuals weighing the trade-offs between the benefits of these technologies and privacy concerns. Effective privacy management is supported by these risk-benefit practices, which aid in making informed data-sharing decisions. The findings suggest that integrating risk-benefit analysis into educational training could help enhance youths' ability to make informed choices. By promoting practical tools and using real-life examples, such programs can help individuals develop a more nuanced understanding about how to balance convenience and privacy risks when using AI systems.

D. Transparency and Trust (TT) Influences Data Control

Transparency and Trust (TT) was found to have a significant positive effect on Data Ownership and Control (DOC). These findings highlight the importance of clear and accessible communication in privacy management. The construct's reliability metrics (AVE = 0.449, CR = 0.686) suggest room for improvement in conceptualizing TT's role in empowering individuals. Transparent practices, such as simplified disclosures and privacy summaries tailored to youths, can enhance understanding and trust, ultimately reducing boundary turbulence. While transparency helps mitigate data-sharing practices, additional tools that allow users to visualize and adjust their privacy settings in real-time could further empower them to take control over their data.

E. Education and Awareness (EA) as the Strongest Predictor of DOC among all factors

EA emerged as the strongest predictor of DOC, underscoring the transformative potential of knowledge in privacy management. Youths who are well-informed about AI systems and data privacy issues demonstrate greater control over their personal data, reaffirming the role of education in enabling effective boundary regulation. The study highlights the need for comprehensive educational programs that combine theoretical learning with hands-on training. By integrating practical applications, such as interactive sessions and real-world problem-solving activities, these programs can help youths internalize privacy principles and implement them effectively in their daily lives.

F. Theoretical Implications

This study advances privacy research by applying the principles of boundary regulation to the context of youth interactions with AI technologies. It highlights the dynamic interplay between education, parental influence, risk perception, and transparency in shaping privacy behaviors. The findings suggest that collaborative frameworks, where knowledge and trust are central, can reduce boundary turbulence and enhance privacy management. Policymakers and system designers should focus on creating environments that empower users with customizable tools and accessible privacy settings. For educational initiatives, integrating risk evaluation and boundary-setting concepts can provide youths with a stronger foundation for managing their privacy in AI-driven ecosystems.

G. Limitations and Future Works

Our study faces some limitations that affect the generalizability and depth of the findings. The use of purposive sampling and a focus on three distinct stakeholder groups, young digital citizens, parents/educators, and AI professionals, may not fully represent the broader population, limiting the generalizability to other demographic groups such as non-technical users or policymakers. Additionally, the cross-sectional design only offers a snapshot in time, constraining our ability to make causal inferences and capture the evolving nature of privacy attitudes and behaviors. Future research could benefit from employing random sampling methods and longitudinal designs to validate these results across a more diverse range of populations. Additionally, the moderate reliability of some constructs, particularly Trust and Transparency (TT) with an AVE of 0.449 and a CR of 0.686, suggests a need for methodological refinement to more accurately capture the complexities of privacy management behaviors within AI contexts. This approach would strengthen

the results and help provide a more in-depth comprehension of the societal applications of CPM concepts.

VI. Conclusion

This study applied CPM theory to examine the privacy perspectives of young digital citizens, parents/educators, and AI developers/researchers using five key validated constructs: Data Ownership and Control (DOC), Parental Data Sharing (PDS), Perceived Risks and Benefits (PRB), Transparency and Trust (TT), and Education and Awareness (EA). Data was collected using survey instruments, refined with a pilot study, and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The resulting model shows that EA significantly influences DOC and PRB, underscoring the critical importance of privacy education in facilitating more effective boundary management strategies. Similarly, TT positively influences DOC, reinforcing the role of transparency in building trust and reducing boundary turbulence. However, the minimal mediation of PRB and the negative effect of PDS on DOC underscore the complexity of privacy behaviors, suggesting external factors like parental dynamics and usability concerns may play critical roles. These results emphasize the need for user-centric privacy controls, tailored transparency mechanisms, and collaborative educational initiatives to empower stakeholders and reduce privacy risks. While this research advances the application of CPM Theory to AI contexts, future studies should expand demographic diversity, refine constructs for improved reliability, and explore longitudinal shifts in privacy behaviors to further inform privacy-centric AI system designs.

Acknowledgment

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. This project has also received funding support from the VIURAC Publish Grant.

References

[1] K. Thai *et al.*, "Perspectives of youths on the ethical use of artificial intelligence in health care research and clinical care," *JAMA Netw Open*, vol. 6, no. 5, pp. e2310659–e2310659, May 2023, doi: 10.1001/JAMANETWORKOPEN.2023.10659.

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

[3] E. Durall Gazulla *et al.*, "Youth perspectives on technology ethics: analysis of teens' ethical reflections on AI in learning activities," *Behaviour & Information Technology*, pp. 1–24, May 2024, doi: 10.1080/0144929X.2024.2350666.

[4] S. Petronio and I. Altman, "Boundaries of Privacy: Dialectics of Disclosure," *Boundaries of Privacy: Dialectics of Disclosure*, Jun. 2023, doi: 10.1353/BOOK4588.

[5] S. Livingstone, "Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family," *Computers, Phones, and the Internet: Domesticating Information Technology*, Mar. 2006, doi: 10.1093/ACPROF:OSO/9780195312805.003.0010.

[6] M. Madden *et al.*, "Teens, social media and privacy," in *Pew Research Center*, Cham: Springer International Publishing, 2013. doi: 10.1007/978-3-030-82786-1_7.

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

[8] Y. J. Park, "Digital Literacy and Privacy Behavior Online," *Communic Res*, vol. 40, no. 2, pp. 215–236, Apr. 2013, doi: 10.1177/0093650211418338/ASSET/IMAGES/LARGE/10.1177_0093650211418338-FIG2.JPEG.

[9] J. Byrne, D. Kardefelt-Winther, S. Livingstone, and M. Stoilova, "Global kids online research synthesis, 2015–2016," *UNICEF Office of Research Innocenti*, no. November, pp. 1–14, 2016, [Online]. Available: http://blogs.lse.ac.uk/gko/

[10] MediaSmarts, "Young Canadians in a wired world, phase III: Life online," Ottawa, 2022.

[11] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, Jan. 2015, doi: 10.1126/SCIENCE.AAA1465.

[12] S. Youn, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach," *J Broadcast Electron Media*, vol. 49, no. 1, pp. 86–110, Mar. 2005, doi: 10.1207/s15506878jobem4901_6.

[13] S. Youn, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *Journal of Consumer Affairs*, vol. 43, no. 3, pp. 389–418, Sep. 2009, doi: 10.1111/J.1745-6606.2009.01146.X.

[14] C. Jensen and C. Potts, "Privacy policies as decision-making tools," pp. 471–478, Apr. 2004, doi: 10.1145/985692.985752.

[15] C. L. Miltgen and D. Peyrat-Guillard, "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries," *European Journal of Information Systems*, vol. 23, no. 2, pp. 103–125, Mar. 2014, doi: 10.1057/ejis.2013.17.

[16] M. Stoilova, S. Livingstone, and R. Nandagiri, "Children's data and privacy online: Growing up in a digital age," *London School of Economics and Political Science.*, no. January, pp. 1–47, 2019.

[17] D. Lyon, "Surveillance, transparency, and trust," *Trust and Transparency in an Age of Surveillance*, pp. 243–257, Jan. 2021, doi: 10.4324/9781003120827-18/SURVEILLANCE-TRANSPARENCY-TRUST-DAVID-LYON.

[18] A. Marwick, "Social privacy in networked publics: Teens' attitudes, practices, and strategies," in *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, 2011.

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

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

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

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

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

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

[25] 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/ASSET/71F5F6E2-6910-455E-987B-54B965DB3990/ASSETS/293411.293475.FP.PNG.

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

[27] 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.

[28] R. C. Mayer, J. H. Davis, and F. D. Schoorman, “An integrative model of organizational trust,” *The Academy of Management Review*, vol. 20, no. 3, p. 709, Jul. 1995, doi: 10.2307/258792.

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

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

[31] 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.

[32] PuhakainenPetri and SiponenMikko, “Improving employees’ compliance through information systems security training,” *MIS Quarterly*, Dec. 2010, doi: 10.5555/2017496.2017502.

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

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

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

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

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

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

[39] W. W. Chin, R. A. Peterson, and S. P. Brown, “Structural equation modeling in marketing: Some practical reminders,” *Journal of Marketing Theory and Practice*, vol. 16, no. 4, pp. 287–298, Sep. 2008, doi: 10.2753/MTP1069-6679160402.

[40] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, “Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research,” *European Business Review*, vol. 26, no. 2, pp. 106–121, 2014, doi: 10.1108/EBR-10-2013-0128.

[41] 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 Administration Review*, vol. 9, no. 4, pp. 395–420, 2012, doi: 10.1590/s1807-76922012005000006.

[42] D. Gefen, D. Straub, and M.-C. Boudreau, “Structural equation modeling and regression: Guidelines for research practice,” *Communications of the Association for Information Systems*, vol. 4, p. undefined-undefined, 2000, doi: 10.17705/1CAIS.00407.

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

[44] A. K. Shrestha and S. Joshi, “Toward ethical AI: A qualitative analysis of stakeholder perspectives,” in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, 2025.