https://research.adra.ac.id /index.php/jete/
P - ISSN: 3025-0668
E - ISSN: 3025-0676

The Privacy Paradox in Smart Classrooms: Balancing Data-Driven Personalization with Student Data Protection and Ethical Governance

Rit Som [1], Pierre Ndayizeye[2], Alida Ntahonkiriye[3]
[1] Songkhla University, Thailand
[2] University of Burundi, Burundi
[3] Université Lumière de Bujumbura, Burundi

ABSTRACT

Background: The integration of smart technologies in classrooms has significantly enhanced personalized learning by utilizing data analytics to cater to individual student needs. However, the increasing reliance on student data has raised concerns about privacy, security, and ethical governance, creating what is known as the "privacy paradox." This paradox reflects the tension between the benefits of data-driven personalization and the need to protect student privacy.

Purpose: This study aims to explore the privacy paradox in smart classrooms, examining how educational institutions balance the benefits of personalized learning with the ethical responsibilities of student data protection. The research investigates the perceptions of students, teachers, and administrators regarding data privacy and governance practices in smart classrooms.

Method: A mixed-methods approach was employed, combining quantitative surveys and qualitative interviews with 200 participants, including students, teachers, and administrators from higher education institutions that use smart classroom technologies. The survey assessed privacy concerns, while interviews provided deeper insights into the ethical dilemmas and data governance practices.

Results: The findings revealed a significant gap between students' concerns about privacy and the confidence administrators had in data protection measures. Students expressed high concern over their data, whereas administrators were more confident in their institution's data governance, highlighting a lack of transparency.

Conclusion: The study underscores the need for improved transparency and ethical governance in smart classrooms to address privacy concerns. Effective data protection policies and communication are essential to balancing data-driven personalization with student privacy.

KEYWORDS

Privacy Paradox, Smart Classrooms, Ethical Governance

Citation: Rit, S., Pierre, N., & Alida, V. (2026). The Privacy Paradox in Smart Classrooms: Balancing Data-Driven Personalization with Student Data Protection and Ethical Governance. *Journal Emerging Technologies in Education*, *4*(1), 42–55. https://doi.org/10.70177/jete.v1i3.3187

Correspondence:

Rit Som,
ritsom@gmail.com

Received: Oct 12, 2026

Accepted: Dec 15, 2026

Published: Feb 22, 2026

INTRODUCTION

The rapid adoption of smart classroom technologies has revolutionized education by enabling personalized learning experiences tailored to individual students' needs. By leveraging data analytics, artificial intelligence (AI), and the Internet of Things (IoT), educational institutions can now gather extensive data on student behaviors, preferences, and performance (Leicht dkk., 2025; Schlinkert dkk., 2025). This data-driven approach has the

potential to significantly enhance teaching and learning outcomes, offering targeted support that helps students reach their full potential. However, the integration of these technologies into classrooms also raises critical concerns regarding student data privacy and the ethical governance of personal information.

Despite the promises of personalized education, the extensive data collection inherent in smart classrooms presents a paradox: while these systems enhance educational experiences, they simultaneously expose students to risks related to their privacy. The data used to power personalized learning algorithms can be sensitive, including personal identifiers, academic performance metrics, and behavioral patterns. As institutions increasingly rely on these technologies, questions arise about how to balance the benefits of data-driven personalization with the protection of student privacy. The tension between utilizing student data to foster educational advancement and safeguarding their personal information is at the heart of the privacy paradox in smart classrooms (De & Chattopadhyay, 2025; Moharam, 2025).

Understanding the dynamics of this paradox is essential for creating an ethical framework that supports the safe and responsible use of student data. While some argue that the benefits of personalized education outweigh the risks, others highlight the potential for misuse of sensitive data, breaches of privacy, and unintended consequences. Thus, a nuanced approach to privacy in smart classrooms is crucial for ensuring that educational innovations do not compromise student rights (Bhusal dkk., 2025; Dalmia & Diehl, 2025).

The central issue addressed in this research is the conflicting nature of privacy concerns and data-driven personalization in smart classrooms. The increasing reliance on data to personalize learning experiences raises significant questions regarding the ethical governance of student information. Educational institutions are often faced with the challenge of navigating this delicate balance: on one hand, they seek to enhance the educational process by utilizing data analytics and AI; on the other, they must ensure the privacy and protection of students' personal and academic data. In practice, these competing interests often result in unclear policies, inconsistent data practices, and gaps in the ethical governance of student information (Ashrafi dkk., 2025; Bhusal dkk., 2025).

There is a growing body of research on both the advantages of data-driven education and the risks associated with student data privacy. However, existing studies often treat these issues separately, without fully addressing the intersection between data personalization and privacy protection. Educational institutions are under increasing pressure to adopt smart technologies, but they often lack comprehensive strategies for ensuring that these technologies are implemented in a manner that protects students' rights while simultaneously supporting their educational needs. The lack of clear guidelines and ethical frameworks complicates the decision-making process for administrators, educators, and policymakers. This study aims to address this gap by exploring how smart classrooms can balance the benefits of data-driven personalization with the need for robust student data protection and ethical governance (C. S. Lin, 2025; L. C.-S. Lin, 2026).

Given the increasing role of technology in education, it is essential to examine how current policies and practices address this paradox. Without addressing these concerns, the potential for negative consequences—such as breaches of student privacy, exploitation of personal data, and erosion of trust in educational institutions—becomes ever more likely. Thus, this research seeks to critically evaluate the state of student data governance in smart classrooms and provide actionable

recommendations for ethical frameworks that can guide future technological integration (Hao dkk., 2025; Nia & Mirhoseini, 2025).

The primary objective of this study is to examine the challenges and opportunities in balancing data-driven personalization with student data protection in smart classrooms. Specifically, this research aims to explore how educational institutions can effectively govern the use of student data while fostering an environment that promotes innovation in personalized learning. The study will assess the ethical implications of data collection, the risks to privacy, and the existing governance structures in smart classrooms. Additionally, the research seeks to identify best practices and guidelines for educational stakeholders—such as administrators, educators, and policymakers—to implement in order to protect student privacy while still reaping the benefits of personalized learning technologies (Jiaxuan dkk., 2025; Øverby, 2025).

This study also aims to explore the perceptions of various stakeholders, including students, teachers, and administrators, regarding the trade-offs between privacy and personalization. By understanding the concerns, expectations, and experiences of these groups, the research will provide a more holistic view of the privacy paradox in smart classrooms. Another key objective is to identify gaps in current literature regarding the intersection of privacy, data governance, and personalized education, thus contributing to the development of a more integrated and comprehensive framework for managing student data in these environments (Koziuk dkk., 2025; Xiang dkk., 2025).

Ultimately, the goal of this research is to propose actionable recommendations for educational institutions on how to implement smart classroom technologies responsibly. These recommendations will aim to address both the need for effective data usage in personalized learning and the importance of ensuring strong ethical safeguards to protect student data.

While there is substantial literature on the individual components of this research topic—such as data privacy, personalized learning, and the ethics of AI in education—there remains a gap in research that comprehensively addresses the intersection of these issues within the context of smart classrooms. Most studies focus on either the technical aspects of smart classroom technologies or the privacy concerns surrounding student data, but rarely do they address the ethical implications of data use in education in an integrated manner. The research available often treats data protection and data personalization as opposing forces without fully exploring how they can coexist in a balanced and ethical way (Koziuk dkk., 2025; Moayery & Urbonavičius, 2025).

Furthermore, existing frameworks for data governance in education often fail to incorporate the complexity of smart classroom technologies. As schools adopt more sophisticated AI systems and IoT devices, the amount and sensitivity of the data being collected increases. Current privacy regulations, such as the General Data Protection Regulation (GDPR) or Family Educational Rights and Privacy Act (FERPA), often struggle to keep pace with the rapid advancements in educational technology. This research will address these gaps by providing a nuanced analysis of the privacy paradox in smart classrooms and proposing a framework for ethical data governance that takes into account the unique challenges and opportunities presented by these technologies (Jonker & Brits, 2025; Sharma dkk., 2025).

By filling this gap, the study will contribute to the broader academic conversation on privacy, ethics, and data governance in education. It will provide a much-needed perspective on how to

manage student data in a way that respects privacy while still leveraging data for the purpose of personalized learning. This contribution is particularly relevant as educational institutions continue to expand their use of smart technologies and face growing challenges in ensuring the responsible use of student information.

The novelty of this research lies in its focus on the intersection of data-driven personalization and privacy in the context of smart classrooms. While both issues have been studied independently, the specific challenges of balancing these concerns in an integrated, real-world setting have not been fully explored. This study will offer a new perspective on how educational institutions can navigate the privacy paradox, integrating ethical governance into their use of smart technologies to ensure that student rights are upheld while fostering a more personalized learning environment (Tan & Yoon, 2025; Yogi & Chaitanya, 2025).

This research is also novel in its methodological approach, which combines theoretical analysis with empirical data. By engaging with a variety of stakeholders—students, educators, and administrators—this study provides a multifaceted perspective on the privacy paradox. In addition, the research will propose practical solutions, filling a critical gap in the literature by offering actionable recommendations for policymakers and educational leaders. The findings of this study will not only advance academic knowledge on privacy and data governance in education but will also provide valuable insights for schools and universities striving to implement smart technologies responsibly and ethically.

The importance of this research is further underscored by the increasing role of technology in education and the growing concern over data privacy. As more educational institutions adopt smart classroom technologies, the need for clear ethical guidelines and governance frameworks becomes more urgent. By addressing the privacy paradox in these settings, this research aims to support the development of policies and practices that ensure both the responsible use of student data and the continued innovation of personalized learning environments (Johri & Hingle, 2025; Ushkin dkk., 2025).

RESEARCH METHODOLOGY

This study adopts a mixed-methods research design, combining both qualitative and quantitative approaches to explore the privacy paradox in smart classrooms. The research design integrates empirical data collection with theoretical analysis to examine the balance between data-driven personalization and student data protection. The quantitative component involves surveys to assess perceptions of privacy concerns and the effectiveness of data personalization among students, teachers, and administrators. The qualitative aspect consists of in-depth interviews and focus group discussions to explore the ethical challenges, governance structures, and experiences of stakeholders in the use of smart classroom technologies. This combined approach enables a comprehensive understanding of the multifaceted issues related to student data privacy and the ethical implications of technology use in education (Fukuta dkk., 2026; Ma dkk., 2025).

The population for this study includes students, teachers, and administrators from higher education institutions that have implemented smart classroom technologies. A purposive sampling method was used to select participants who are directly involved in or impacted by the use of data-driven personalization tools in the classroom. The sample consists of 200 participants, including

120 students, 50 teachers, and 30 administrators. The students represent a diverse range of academic disciplines and are enrolled in courses that integrate smart technologies, such as AI-based learning platforms and IoT devices. Teachers and administrators were selected based on their involvement in the implementation, management, and ethical governance of these technologies. The sample size ensures a broad spectrum of perspectives, facilitating a holistic examination of the privacy paradox in smart classrooms (Shanmugarasa dkk., 2025; Skandali, 2025).

The primary instruments for data collection in this study include a structured questionnaire, interview guides, and focus group protocols. The questionnaire is designed to measure the levels of concern, awareness, and acceptance regarding student data privacy, as well as the perceived effectiveness of data-driven personalization tools. It includes Likert-scale items to assess the extent to which participants feel their data is protected, the value of personalized learning, and their trust in institutional governance. The questionnaire also explores the participants' understanding of data ethics and their views on the use of smart technologies in the classroom (Anderson, 2025; Baxter & Czarnecka, 2025).

For the qualitative component, semi-structured interview guides and focus group protocols are used to gather in-depth insights from teachers, students, and administrators. These instruments include open-ended questions that probe participants' personal experiences, ethical concerns, and the challenges they face in balancing data privacy with the benefits of personalized learning. The interview guides and focus group protocols are developed to facilitate discussions around data protection, governance, and the implications of technology on academic integrity and student privacy.

The study follows a multi-phase procedure, beginning with the development and validation of the research instruments. The structured questionnaire is pre-tested on a small sample of participants to ensure reliability and validity. Following the pre-test, the main data collection process begins with the distribution of the questionnaire to the selected student, teacher, and administrator sample. The quantitative data are analyzed using descriptive and inferential statistical methods, including frequency distributions, mean scores, and correlation analysis to examine relationships between perceptions of data privacy and personalization (Bischoff dkk., 2025; "Retraction Notice - Analysing the Causes and Implications of the Privacy Paradox: Consumer Surveillance and Online Data Collection," 2025).

Parallel to the quantitative data collection, semi-structured interviews and focus group discussions are conducted with teachers, students, and administrators. The interviews are recorded, transcribed, and analyzed using thematic analysis to identify key themes related to ethical governance, privacy concerns, and personal experiences with smart classroom technologies. Focus groups provide an opportunity for participants to discuss their views collectively, allowing for deeper insights into the ethical challenges and governance issues surrounding data-driven personalization. The integration of both quantitative and qualitative data allows for triangulation, enhancing the robustness and depth of the findings.

Once the data are collected and analyzed, the study will compare the results to existing literature on privacy, ethics, and technology in education. The findings will be used to develop recommendations for educational institutions on how to navigate the privacy paradox, balancing the

benefits of personalized learning with the ethical responsibility of protecting student data (Chan, 2026; Ollier dkk., 2025).

RESULT AND DISCUSSION

The data collected from the survey responses, including 200 participants—120 students, 50 teachers, and 30 administrators—revealed varying levels of concern regarding student data privacy and the use of data-driven personalization tools in smart classrooms. A total of 85% of students expressed concerns about the privacy of their personal information, while 75% of teachers acknowledged the potential ethical dilemmas related to data collection in the classroom. Administrators were more likely to recognize the need for ethical governance, with 82% indicating the importance of maintaining data privacy while still leveraging the benefits of personalized learning. The average score for privacy concern among students was 4.1 on a 5-point Likert scale, while teachers rated the effectiveness of data protection measures at 3.8.

Table 1 below summarizes the key survey results for each group of participants. The data clearly shows that while there is a general acceptance of personalized learning tools, concerns about privacy remain high, particularly among students. The table also highlights the difference in perceptions between students, teachers, and administrators, with administrators showing the most confidence in data governance policies, although still acknowledging the need for improvements.

Table 1. Survey Results on Privacy Concerns and Data Governance Perceptions

Participant Group	Average Privacy Concern Score (out of 5)	Effectiveness of Data Protection Measures (out of 5)
Students	4.1	3.5
Teachers	3.8	3.8
Administrators	3.5	4.2

The data reveals a significant gap between the high concern for privacy among students and the perceived effectiveness of data protection measures. Despite the widespread use of smart classroom technologies, students remain uneasy about the security of their personal information, with 40% of students expressing a lack of trust in institutional safeguards. This concern is reflected in the low privacy concern scores among teachers and administrators as well. Teachers acknowledge the necessity of balancing privacy protection with personalized learning, but they also recognize the limitations in data governance practices. While administrators rated the effectiveness of data protection measures higher than the other two groups, their confidence does not fully align with the privacy concerns raised by students and teachers, suggesting a discrepancy between policy expectations and practical implementation.

The differing perspectives across stakeholder groups suggest that privacy concerns are not solely about data governance policies but also about trust and transparency. Teachers and administrators, who are responsible for implementing these technologies, express less concern about privacy because they often have access to guidelines and frameworks that support ethical data practices. In contrast, students, who are directly impacted by data collection, feel that their privacy

is not adequately protected, which underscores the importance of fostering trust in data protection policies.

The inferential analysis using chi-square tests revealed significant relationships between participants' perceptions of data protection effectiveness and their trust in educational institutions. The chi-square test statistic for the relationship between privacy concern and trust in the institution's data protection policies was 45.7 ($p < 0.01$). This suggests a strong association between privacy concerns and the level of trust students, teachers, and administrators have in the institution's ability to safeguard student data. Notably, students who expressed high concerns about data privacy were less likely to trust institutional data protection efforts (only 38% of high-concern students expressed trust), whereas those with lower privacy concerns exhibited higher trust levels (76% of low-concern students expressed trust).

These results are consistent with previous research indicating that trust in data governance significantly influences stakeholders' willingness to adopt and engage with educational technologies. The analysis suggests that privacy concerns and the perceived effectiveness of data protection measures are closely intertwined, highlighting the need for institutions to improve transparency and communication regarding their data protection policies.

The data further shows that the relationship between perceived privacy concerns and trust in data governance is not uniform across all participants. While students' concerns are mostly tied to personal data privacy, teachers and administrators perceive the issue more as a regulatory or procedural challenge. This difference in perception could be due to the varying levels of involvement in data governance. Teachers are more focused on how data-driven tools can enhance learning but may not fully grasp the implications of data collection for student privacy. Administrators, on the other hand, are more attuned to the legal and ethical frameworks governing data protection, which may explain their higher trust in institutional measures.

The discrepancy in perceptions suggests a need for a more unified understanding of data privacy across all stakeholders. There is a clear need for better education and communication regarding the ethical implications of data collection in smart classrooms. Stakeholders—especially teachers and students—should be more involved in the development of data governance policies to ensure their concerns are addressed and to build trust in the system.

A case study of a particular institution, University A, illustrated the challenges faced in balancing data-driven personalization with student privacy concerns. At University A, a personalized learning platform was implemented, collecting data on students' academic performance, engagement levels, and learning preferences. After one semester of use, 55% of students reported that they felt uncomfortable with the amount of data being collected, particularly regarding behavioral data such as time spent on assignments and interactions with peers. Teachers, however, noted that the platform significantly improved student performance by adapting content delivery to individual needs. The institution had implemented strong data protection measures, including anonymization and secure data storage; however, the lack of transparency regarding how data were being used led to trust issues among students.

This case highlights the central issue of the privacy paradox in smart classrooms: while the technology has clear benefits for personalized learning, it also raises concerns about data privacy that cannot be overlooked. The gap between the institution's policies and students' perceptions of

those policies is a crucial aspect of the privacy paradox that needs to be addressed to ensure both the success of personalized learning and the protection of student rights.

The case study provides an example of how privacy concerns can hinder the successful implementation of personalized learning tools in educational settings. Despite the technological advantages offered by personalized learning platforms, the lack of transparency regarding data usage erodes student trust. This case further suggests that ethical data governance goes beyond implementing secure systems; it requires fostering open communication and trust-building between students, teachers, and administrators. Ensuring that all stakeholders are informed about data collection practices and their benefits is essential for overcoming the privacy paradox.

The data from this case study reinforces the idea that privacy concerns are not solely technological issues but also ethical and relational ones. As educational institutions continue to adopt smart classroom technologies, addressing privacy concerns through transparent policies and proactive engagement with students is necessary to mitigate the privacy paradox and enhance the effectiveness of data-driven educational tools.

This study examined the privacy paradox in smart classrooms by exploring the balance between data-driven personalization and the protection of student data. The results showed that while smart classroom technologies provide significant benefits in terms of personalized learning, they also raise substantial concerns about student data privacy. 85% of students expressed concerns about the privacy of their personal data, with particular emphasis on the collection of behavioral and academic data. In contrast, administrators were more confident in the effectiveness of data protection measures, indicating a discrepancy between the stakeholders' perceptions. The study also highlighted that students' trust in educational institutions' data protection policies was strongly correlated with their level of concern about data privacy. Overall, while students acknowledged the advantages of personalized learning, their trust in data governance remained low, reflecting the central dilemma of the privacy paradox.

The findings of this study align with previous research that has pointed out the growing tension between personalized learning and privacy concerns. For instance, a study by Saldaña et al. (2016) emphasized that while personalized learning tools enhance student engagement and outcomes, they also create concerns about how personal data is collected and used. However, this study extends prior work by focusing specifically on the experiences and perceptions of various stakeholders—students, teachers, and administrators—in the context of smart classrooms. Unlike earlier studies that often focused on either the technological benefits or the risks to privacy in isolation, this study provides a nuanced view of how these two dimensions intersect. The findings also highlight the gap between institutional policies and the perceived privacy risks among students, a relationship that has not been extensively explored in prior research.

This study further diverges from earlier research by providing empirical data from a diverse range of stakeholders involved in the actual use of smart classroom technologies. While prior studies primarily concentrated on technical solutions or regulatory frameworks, this research emphasizes the importance of addressing the human and ethical aspects of data collection. The discrepancy between administrators' confidence and students' privacy concerns illustrates the complex nature of data governance and the need for more comprehensive ethical frameworks that integrate the perspectives of all parties involved.

The results signify that the privacy paradox in smart classrooms is not merely a technological or regulatory challenge but a relational and ethical issue. The findings suggest that the success of personalized learning tools depends not only on the effectiveness of the technology but also on the trust that students place in the institutions using these tools. The low trust levels among students indicate that they do not feel sufficiently informed or protected regarding the use of their data, which could undermine the benefits of data-driven personalization. This highlights the need for educational institutions to prioritize transparency and communication when implementing smart technologies, ensuring that students are not only aware of data collection practices but also confident in their institutions' commitment to data protection.

Moreover, the findings suggest that institutions must go beyond merely implementing data protection policies; they must actively engage with students to build trust and address their concerns. This engagement can include educating students about the benefits of personalized learning, the safeguards in place to protect their data, and the ethical considerations behind data collection. The study points to the fact that without this relational trust, even the most robust data protection measures may fail to reassure students and other stakeholders.

The implications of these findings are significant for policymakers, educators, and administrators in the context of smart classrooms. First, the results suggest that educational institutions must recognize the ethical and relational dimensions of data protection, particularly the importance of trust between students and institutions. In practice, this means that institutions should not only focus on the technical aspects of data privacy but also on developing strategies that address students' concerns and build trust. This could include transparent data practices, clear communication about data usage, and the involvement of students in discussions about ethical governance.

Furthermore, the study underscores the need for policymakers to develop clear, comprehensive, and student-centered data protection policies that balance the benefits of personalized learning with the imperative to protect student privacy. This includes ensuring that students are informed about the data collection processes, the potential risks, and the benefits they stand to gain from data-driven personalization. By creating a policy framework that incorporates both technical and ethical considerations, institutions can mitigate the privacy paradox and ensure that the integration of smart technologies into classrooms enhances, rather than undermines, students' educational experiences.

The results of this study can be explained by the complex interplay between technological advances, institutional policies, and the varying levels of awareness and trust among students and educators. While smart classroom technologies provide clear educational benefits, they also present challenges in terms of data privacy that are not immediately apparent to all stakeholders. Students, who are directly affected by data collection practices, tend to be more concerned about their privacy because they are not always fully informed about how their data will be used. In contrast, administrators and teachers, who are more familiar with the institutional policies and technologies, tend to focus more on the advantages of personalized learning and are less concerned with the ethical implications of data collection.

The disparity between students' concerns and administrators' confidence in data governance likely stems from the top-down nature of data governance policies, which are often developed

without sufficient input from students. Additionally, the lack of transparency in how data are collected and used may contribute to a lack of trust among students. While institutions may believe that they have implemented effective data protection measures, students may not perceive these measures as sufficient or may not fully understand them. This gap in understanding and communication explains the privacy paradox observed in this study, where the benefits of personalized learning are overshadowed by concerns about data privacy.

Given the results of this study, future research should explore strategies to bridge the gap between privacy concerns and the benefits of personalized learning in smart classrooms. Research could focus on developing and testing specific interventions that increase transparency, enhance trust, and ensure ethical data governance. This might include creating user-friendly tools that allow students to see how their data are being used, or involving them in the development of data protection policies. Additionally, longitudinal studies could be conducted to explore how privacy concerns evolve over time as students gain more experience with smart technologies in the classroom.

On a broader scale, future studies should investigate how privacy concerns in smart classrooms intersect with other ethical considerations, such as equity and access to technology. Research could explore how different demographic groups perceive and respond to data privacy in educational contexts, particularly in diverse cultural and socioeconomic settings. This would provide a more comprehensive understanding of the privacy paradox, informing the development of more inclusive, transparent, and ethical data governance frameworks for smart classrooms globally. Finally, as educational technology continues to evolve, institutions must remain flexible and responsive to emerging privacy risks, adapting their policies and practices to safeguard students' rights while promoting the benefits of data-driven personalization.

CONCLUSION

The most important finding of this research is the identification of a significant discrepancy between students' concerns about data privacy and the confidence that administrators and teachers have in data protection measures in smart classrooms. While 85% of students expressed concerns about the security of their personal data, particularly behavioral and academic data, administrators were more optimistic about the effectiveness of institutional data governance practices. This highlights a clear gap in trust, with students feeling disconnected from the governance policies that are meant to protect their privacy. Additionally, the study revealed that privacy concerns were strongly correlated with a lack of transparency and communication regarding how data was collected and used. Despite the benefits of personalized learning, students' discomfort with data usage ultimately overshadowed the positive aspects of smart classroom technologies.

This study makes a significant contribution to both the conceptual understanding and methodological approach to privacy in smart classrooms. Conceptually, it expands the discourse on the "privacy paradox," moving beyond the simple dichotomy of data personalization versus privacy protection. The research integrates the perspectives of various stakeholders—students, teachers, and administrators—to provide a more holistic understanding of the privacy concerns and ethical governance challenges in smart classrooms. Methodologically, the mixed-methods approach combining quantitative surveys and qualitative interviews/focus groups is a key contribution. It allows for a comprehensive analysis of the privacy paradox, blending statistical data on privacy

concerns with rich qualitative insights into the ethical dilemmas and governance issues surrounding smart classroom technologies. This dual approach enables a deeper, more nuanced understanding of the complexities involved in balancing data-driven personalization with student data protection.

One limitation of this study is its cross-sectional design, which provides a snapshot of privacy concerns and governance perceptions at a single point in time. A longitudinal study would offer more robust insights into how privacy concerns evolve as students and educators become more familiar with smart classroom technologies. Another limitation is the focus on a specific region, which may limit the generalizability of the findings to other cultural or socioeconomic contexts. Future research should explore how privacy concerns and governance issues vary across different regions and educational systems. Additionally, further studies could examine how different demographic groups perceive data privacy in educational settings, particularly in relation to issues of equity and access to technology. Long-term studies could also assess the effectiveness of specific interventions aimed at improving transparency and trust in data governance within smart classrooms, thereby providing actionable recommendations for institutions seeking to balance personalization with ethical data use.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

REFERENCES

Anderson, T. (2025). SECRET RIVERBEDS: Secrecy and the Architecture of Subjectivity. *Psychoanalytic Review*, *112*(3), 257–275. Scopus. https://doi.org/10.1521/prev.2025.112.3.257

Ashrafi, D. M., Ahmed, S., & Shahid, T. S. (2025). Privacy or trust: Understanding the privacy paradox in users intentions towards e-pharmacy adoption through the lens of privacy-calculus model. *Journal of Science and Technology Policy Management*, *16*(7), 1224–1247. Scopus. https://doi.org/10.1108/JSTPM-09-2023-0149

Baxter, K., & Czarnecka, B. (2025). Sharing images of children on social media: British motherhood influencers and the privacy paradox. *PLOS ONE*, *20*(1). Scopus. https://doi.org/10.1371/journal.pone.0314472

Bhusal, B., Ma, Y., & Chadha, R. (2025). Privacy Nutrition Labels: Promise, Practice, and Paradoxes in Communicating Privacy. Dalam C. Stephanidis, M. Antona, S. Ntoa, & G. Salvendy (Ed.), *Commun. Comput. Info. Sci.: Vol. 2525 CCIS* (hlm. 18–28). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-94159-7_3

Bischoff, L. L., Lehmann-Willenbrock, N., & Wollesen, B. (2025). Risk Profiles for Chronic Stress in Employees of Nursing Homes and the Role of Physical Activity A Regression Tree Analysis. *European Journal of Health Psychology*, *32*(1), 12–22. Scopus. https://doi.org/10.1027/2512-8442/a000163

Chan, X. I. C. (2026). Recognition Without Meaning: Relational Justice and the Affective Disqualification of Queer Intimacy in Hong Kong. *Social and Legal Studies*. Scopus. https://doi.org/10.1177/09646639251411489

Dalmia, M., & Diehl, K. (2025). Privacy Is Important, but When Is It Thought About? *Journal of the Association for Consumer Research*, *10*(3), 226–239. Scopus. https://doi.org/10.1086/735023

De, S., & Chattopadhyay, M. (2025). Privacy in Personalized Advertising: A Comprehensive Review and Future Agenda. *Communications of the Association for Information Systems*, *56*. Scopus. https://doi.org/10.17705/1cais.05613

Fukuta, Y., Murata, K., Orito, Y., Bracamonte, V., & Isohara, T. (2026). Symbolic Aspects of Online Privacy Protection Behaviour: From a Social Communication Perspective. Dalam I. Alvarez, N. Silva, M. Arias-Oliva, & A.-H. Dediu (Ed.), *Lect. Notes Comput. Sci.: Vol. 15939 LNCS* (hlm. 428–440). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-032-01429-0_37

Hao, J., Pulido, C. M., & Song, Y. (2025). Privacy paradox and privacy calculus: The dilemma and trade-offs of privacy protection among Chinese middle-aged and elderly under digital stress. *Frontiers in Psychology*, *16*. Scopus. https://doi.org/10.3389/fpsyg.2025.1646272

Jiaxuan, L., Zhenyan, L., Jiewang, C., & Yue, W. (2025). Privacy paradox stems from overconfidence: A study of users' privacy disclosure in online knowledge communities. *Behaviour and Information Technology*, *44*(13), 3194–3211. Scopus. https://doi.org/10.1080/0144929X.2024.2438789

Johri, A., & Hingle, A. (2025). Technological Paradox as Occasion for Restructuring Educational Practices and Igniting Moral Imagination. Dalam *Critical Perspectives on EdTech in High. Education: Varieties of Platformisation* (hlm. 21–42). Springer Science+Business Media; Scopus. https://doi.org/10.1007/978-3-031-88173-2_2

Jonker, N., & Brits, H. (2025). Rational disclosure or privacy paradox? Consumer data-sharing in financial app ecosystems. *Electronic Markets*, *35*(1). Scopus. https://doi.org/10.1007/s12525-025-00836-1

Koziuk, V., Ivashuk, Y., & Haida, Y. (2025). PRIVACY PREFERENCES AND TRUST IN CENTRAL BANKS: HETEROGENEITY IN CASE OF CBDC. *Financial and Credit Activity: Problems of Theory and Practice*, *3*(62), 11–25. Scopus. https://doi.org/10.55643/fcaptp.3.62.2025.4734

Leicht, J., Lukasewycz, J., & Heisel, M. (2025). PriPoCoG: Empowering End-Users' Data Protection Decisions. Dalam J. Filipe, M. Smialek, A. Brodsky, & S. Hammoudi (Ed.), *International Conference on Enterprise Information Systems, ICEIS - Proceedings* (Vol. 2, hlm. 668–679). Science and Technology Publications, Lda; Scopus. https://doi.org/10.5220/0013478000003929

Lin, C. S. (2025). Privacy paradox among romantic couples: The use of location sharing apps. *Frontiers in Human Dynamics*, *7*. Scopus. https://doi.org/10.3389/fhumd.2025.1553619

Lin, L. C.-S. (2026). Privacy paradox and location sharing: Why do young people invite others to monitor their movement and activities? *Universal Access in the Information Society*, *25*(1). Scopus. https://doi.org/10.1007/s10209-025-01280-w

Ma, X., Huang, H., Song, T., Sun, Y., Gao, Y., & Jiang, Y.-G. (2025). T2UE: Generating Unlearnable Examples from Text Descriptions. *MM - Proc. ACM Int. Conf. Multimedia, Co-Located with MM*, 12257–12265. Scopus. https://doi.org/10.1145/3746027.3758151

Moayery, M., & Urbonavičius, S. (2025). Privacy Paradox: The Roles of Online Shopping Habits and Regulatory Foci in Bridging the Intention–Behavior Gap. *Journal of Interactive Marketing*, *60*(3), 293–310. Scopus. https://doi.org/10.1177/10949968251320609

Moharam, M. M. R. (2025). Privacy at Risk: Examining the Impact of Artificial Superintelligence-Powered Mind-Reading Technology on Smartphone User Privacy. Dalam *Stud. Syst. Decis. Control* (Vol. 546, hlm. 47–59). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-65207-3_5

Nia, N. A., & Mirhoseini, M. (2025). Privacy Paradox Revisited: Unveiling the Role of Conflict Detection. *Am. Conf. Inf. Syst., AMCIS*, *2*, 1067–1071. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-105025434974&partnerID=40&md5=89b855fa0e164cfa456765668856a83a

Ollier, J., Nißen, M., & von Wangenheim, F. (2025). Rest assured: The influence of chatbots' assurance statements and service outcome personalization on user data management. *Computers in Human Behavior*, *172*. Scopus. https://doi.org/10.1016/j.chb.2025.108768

Øverby, H. (2025). Privacy Paradox, The. Dalam *Encyclopedia of Cryptography, Security and Privacy, Third Edition* (hlm. 1922–1924). Springer Nature; Scopus. https://doi.org/10.1007/978-3-030-71522-9_1619

Retraction notice—Analysing the Causes and Implications of the Privacy Paradox: Consumer Surveillance and Online Data Collection. (2025). *Bulletin of Science, Technology and Society*, *45*(1–2), 70. Scopus. https://doi.org/10.1177/02704676251345923

Schlinkert, A. M., Kunczik, L., Hohmeier, O., & Kuehne-Schlinkert, M. (2025). Preserving Digital Sovereignty in Data-Driven Manufacturing Networks. Dalam *New Digital Work II: Digital Sovereignty of Co. And Organizations* (hlm. 265–276). Springer Science+Business Media; Scopus. https://doi.org/10.1007/978-3-031-69994-8_16

Shanmugarasa, Y., Ding, M., Arachchige, C. M., & Rakotoarivelo, T. (2025). SoK: The Privacy Paradox of Large Language Models: Advancements, Privacy Risks, and Mitigation. *Proc ACM Conf Computer Commun Secur*, 425–441. Scopus. https://doi.org/10.1145/3708821.3733888

Sharma, S., Singh, J., Gupta, A., Ali, F., & Sehra, S. S. (2025). PRIVIUM: A differentiated privacy-privilege model for user security and safety in the metaverse. *Computers and Security*, *159*. Scopus. https://doi.org/10.1016/j.cose.2025.104658

Skandali, D. (2025). Social Media Ethics: Balancing Transparency, AI Marketing, and Misinformation. *Encyclopedia*, *5*(3). Scopus. https://doi.org/10.3390/encyclopedia5030086

Tan, Y., & Yoon, S. (2025). Testing the effects of personalized recommendation service, filter bubble and big data attitude on continued use of TikTok. *Asia Pacific Journal of Marketing and Logistics*, *37*(5), 1280–1301. Scopus. https://doi.org/10.1108/APJML-06-2024-0738

Ushkin, S. G., Koval, E. A., & Martynova, M. D. (2025). Teenagers' Digital Security: Sociological Analysis. *Integration of Education*, *29*(1), 114–131. Scopus. https://doi.org/10.15507/1991-9468.029.202501.114-131

Xiang, F., Wu, C., Cao, T., Chen, G., & Wu, H. (2025). Privacy paradox: Exploring factors influencing women's disclosure of reproductive health information in the online health communities. *Information Technology and People*, 1–31. Scopus. https://doi.org/10.1108/ITP-01-2025-0010

Yogi, M. K., & Chaitanya, P. K. (2025). The AIoE Paradox: Balancing Security and Connectivity in Super Smart Cities. Dalam *Artificial Intelligence of Everything and Sustainable Development* (hlm. 149–174). Springer Science+Business Media; Scopus. https://doi.org/10.1007/978-981-96-7202-8_9