LIDR
Language, Identity and the Digital Realm
jlid.zand.ac.ir
https://doi.org/10.22034/lidr.2025.722877
1(1), 2025, pp. 1-17

Research Article

Privacy Issues in Online Learning: A Review of Literature and Suggestions for Further Research

Mohammad Aliakbari [1], Pooria Barzan *[2], Mahammad Mahdi Maadikhah [3]

1. Professor, Department of English Language and Literature, Faculty of Humanities, Ilam University, Ilam, Iran.maliakbari@hotmail.com
2*. PhD Candidate, Department of English Language and Literature, Faculty of Humanities, Ilam University, Ilam, Iran. Pooriabarzan@yahoo.com (Corresponding author)
3. PhD student, Department of English Language and Literature, Faculty of Humanities, Ilam University, Iran. m.maadikhah@ilam.ac.ir

ARTICLE INFO

Submission History

Received: 2025-02-20
Accepted: 2025-04-19

Keywords

Privacy
Online learning
E-learning
Learning analytics
Data protection

ABSTRACT

The rapid proliferation of online learning platforms, accelerated by the COVID-19 pandemic, has transformed global education but also raised significant privacy concerns. This literature review synthesizes existing research to explore the multifaceted dimensions of privacy in online learning environments, focusing on (1) prevalent privacy concerns, (2) stakeholders' perspectives toward privacy, (3) strategies and technologies for mitigating privacy risks, and (4) gaps and future directions in research. To address these aims, 24 peer-reviewed articles were systematically analyzed. Key findings reveal pervasive privacy concerns among students and educators, including risks related to unauthorized data access, misuse of personal information, and ethical challenges posed by emerging technologies such as artificial intelligence (AI) and virtual reality (VR). The review also identifies strategies to mitigate privacy risks, such as customizable privacy settings, robust data protection policies, and privacy-enhancing technologies (PETs). However, existing literature lacks focus on specific demographics, longitudinal impacts, and the intersection of privacy and accessibility. The authors argue that transparent policies, ethical practices, and adaptive solutions are critical to creating secure online learning environments. Addressing these challenges is essential to ensuring the benefits of digital education without compromising user privacy and data security.

Introduction

In recent years, online learning has become an integral component of education systems worldwide, driven by advancements in digital technologies and the widespread adoption of internet-based platforms. This shift from traditional face-to-face education to virtual environments has brought significant benefits, including enhanced accessibility, flexibility, and opportunities for personalized learning. Students can access and interact with educational materials from nearly any location, as long as they are connected to the internet. This flexibility makes online learning especially advantageous for non-traditional students, including working professionals and those with familial responsibilities (Karuniawan, 2023; Mawene, 2023; Santoso et al., 2022).

Moreover, the flexibility of online learning allows for personalized educational experiences tailored to individual learning styles and paces. This customization can lead to improved learning outcomes, as students can revisit materials and engage with content in ways that best suit their preferences (Fernando et al., 2022; Sasmita et al., 2021). The integration of various technological tools further enhances engagement by providing interactive and immersive learning experiences. Multimedia resources such as videos, interactive quizzes, and discussion forums cater to diverse learning preferences, thereby increasing student motivation and participation (Ma et al., 2023; Orikana et al., 2022; Syarbini et al., 2022; Wang et al., 2022). However, alongside these advantages, the rapid expansion of online education has also raised critical concerns about privacy and data security.

The proliferation of online learning platforms, especially in response to the COVID-19 pandemic, has significantly transformed educational landscapes. However, this transition has underscored pressing concerns regarding privacy and data protection, as students and educators navigate environments characterized by extensive data collection and analysis. Privacy in online learning encompasses multiple dimensions, including data security, user consent, and the ethical implications of technology use in education. As institutions increasingly rely on digital tools to enhance learning experiences, it is crucial to address the challenges associated with safeguarding student privacy (Cahyanto, 2023; Jiang et al., 2022; Marín et al., 2022).

At its core, privacy in online learning involves protecting personal information and ensuring that learners maintain control over their data. Educational platforms often collect vast amounts of personal data, ranging from basic identification details to more sensitive information such as behavioral patterns, academic performance, and even biometric data. While these data collection practices aim to improve user experience and educational outcomes, they also pose significant risks, including unauthorized access, misuse of personal information, and cybersecurity threats. Consequently, privacy concerns have become a critical issue requiring careful scrutiny and proactive solutions (He, 2022).

Despite the growing body of research on privacy in online education, there remains a notable gap in the literature concerning a comprehensive review that synthesizes these findings. This article seeks to fill that gap by providing an in-depth examination of the

multifaceted dimensions of privacy in online learning environments. Specifically, it aims to identify prevalent privacy concerns and find strategies for mitigating them, exploring stakeholders' perceptions, data protection measures, and the implications for educational practices. By integrating insights from interdisciplinary studies, this review endeavors to offer a holistic understanding of the current state of privacy in online learning and identify areas requiring further investigation.

The literature review is guided by the following key research questions:

1. What are the prevalent privacy concerns in online learning environments?
2. How do different stakeholders (students, educators, institutions) perceive and address privacy in online learning?
3. What strategies and technologies are proposed or implemented to mitigate privacy risks in online learning?
4. What are the identified gaps and future directions in research on privacy in online learning?

By addressing these questions, this review aims to contribute to the ongoing discourse on privacy in digital education and provide valuable insights for educators, policymakers, and researchers striving to create secure and ethical online learning environments.

Methodology

This section outlines the systematic approach adopted for conducting the literature review on privacy in online learning. The methodology ensures a comprehensive and unbiased synthesis of existing research by following a structured process that includes the selection of databases, development of inclusion and exclusion criteria, and analysis of the retrieved studies.

Search Strategy

To identify relevant literature, a systematic search was conducted across multiple academic databases, including but not limited to ScienceDirect, Springer, Wiley, Sage, Taylor & Francis, Oxford, PubMed, Google Scholar, and IEEE Xplore. Search terms were developed based on the research questions and included combinations of keywords and Boolean operators. Examples of search strings used are: "privacy AND online learning," "data protection AND e-learning," "student privacy AND virtual classrooms," and "privacy concerns AND digital education." These search terms were tailored for each database to optimize results and ensure comprehensiveness.

Inclusion and Exclusion Criteria

To ensure relevance and quality, studies were included or excluded based on the following criteria:

Inclusion Criteria:

1. Peer-reviewed journal articles published between 2003 and 2024.
2. Studies explicitly addressing privacy concerns, data protection, or related topics in online learning environments.
3. Articles written in English.

Exclusion Criteria:

1. Studies focused solely on technical aspects of cybersecurity without addressing privacy in an educational context.
2. Articles with insufficient methodological rigor, such as those lacking clear research design or data analysis.

3. Duplicate studies or articles not accessible in full text.

Data Extraction and Synthesis

From the initial searches, over 1,300 abstracts were reviewed, yielding 93 papers for closer examination. Based on the inclusion/exclusion criteria, 24 articles were included and reviewed in detail. The selected studies were assessed using a standardized data extraction form to ensure consistency. The form captured the following information:

- Publication details (author, year, title, and source).
- Study objectives and research questions.
- Key findings related to privacy issues and solutions in online learning.
- Limitations and recommendations for future research.

A thematic analysis was conducted to identify recurring patterns, trends, and gaps in the literature. Thematic coding was performed using qualitative data analysis software (e.g., NVivo) to ensure systematic categorization and comparison across studies.

Quality Assessment

The quality of the included studies was assessed using established frameworks such as the Critical Appraisal Skills Programme (CASP) checklist. This process ensured that only robust and credible research was synthesized in the review. Studies were evaluated based on criteria such as clarity of research aims, appropriateness of methodology, and validity of conclusions.

Ethical Considerations

Although this study involved secondary data analysis, ethical considerations were observed by properly citing all sources and adhering to copyright regulations. The review also considered the potential biases introduced by publication trends and mitigated them by including a diverse range of sources.

By following this methodology, the review provides a rigorous and comprehensive understanding of privacy in online learning, laying the groundwork for future research and practical interventions.

General Overview and results

Privacy Concerns in Online Learning Environments

The rapid proliferation of online learning environments, particularly accelerated by the COVID-19 pandemic, has brought to the forefront a myriad of privacy concerns that affect both students and educators. These concerns are multifaceted, encompassing issues related to data collection, surveillance, ethical use of technology, and institutional accountability. As educational institutions increasingly pivot toward digital platforms, understanding these privacy challenges is crucial for fostering a safe and effective educational experience.

Data Collection and Privacy Risks

One of the primary concerns in online learning environments is the extensive data collection that occurs through various educational technologies. Platforms often gather personal information, including academic performance, engagement metrics, and even biometric data, to enhance learning experiences and tailor educational content to individual needs (Jiang et al., 2022; Marín et al., 2022). However, this datafication raises significant privacy issues, as students may not fully

understand what data is being collected, how it is used, or who has access to it (Alier et al., 2021; Chang, 2021). The implications of such data collection are profound, leading to unauthorized data sharing, breaches of confidentiality, and potential misuse of sensitive information (Cahyanto, 2023). This is particularly concerning in light of the increasing sophistication of cyber threats that target educational institutions (Romansky & Noninska, 2016).

Surveillance Technologies and Student Privacy

In addition to data collection, surveillance technologies used in online learning have sparked considerable debate regarding privacy invasion. The use of webcams and microphones in synchronous online sessions has been identified as a significant source of concern. Almekhled and Petrie (2023) discuss how educators in the UK have reported challenges related to monitoring student participation while simultaneously grappling with privacy issues associated with these technologies. The pressure to maintain engagement can lead to intrusive practices, where students feel compelled to keep their cameras on, thereby compromising their sense of privacy. The fear of being constantly watched can lead to heightened anxiety and discomfort, ultimately impacting students' willingness to engage fully in the learning process (Jiang et al., 2022). Blackmon and Major (2023) further highlight that students express significant apprehension regarding "unwanted images" and the potential for "screenshots that can be taken and shared" during online classes, which can lead to feelings of vulnerability and exposure. Such practices not only violate personal boundaries but also undermine the trust that is essential for effective learning environments.

Ethical Implications of Learning Analytics and AI

Beyond surveillance, the ethical implications of using learning analytics in educational settings cannot be overlooked. Learning analytics involves the collection and analysis of data to improve educational outcomes, but it also raises questions about consent, transparency, and accountability (Liu & Khalil, 2023; Pardo & Siemens, 2014). Students may feel uneasy about how their data is being utilized, particularly if they perceive that the benefits of data collection do not outweigh the risks to their privacy (Jiang et al., 2022; Anwar, 2020). The challenge lies in balancing the need for data-driven insights with the imperative to protect individual privacy rights. Institutions must establish clear policies and practices that prioritize ethical considerations in the use of learning analytics (Reidenberg & Schaub, 2018; Rubel & Jones, 2016).

Moreover, the integration of artificial intelligence (AI) in educational technologies introduces additional layers of complexity regarding privacy. AI systems often rely on vast amounts of data to function effectively, raising concerns about data security and the potential for algorithmic bias (Huang, 2023). While AI can enhance educational experiences through personalization, it also poses significant risks to information security and privacy. Students may be apprehensive about how AI technologies could misinterpret their data or lead to discriminatory practices in educational assessments and feedback (Anwar, 2020; Huang, 2023). As AI continues to evolve, it is

imperative that educational institutions remain vigilant in addressing these privacy concerns and ensuring that AI applications are designed with ethical considerations at their core (Huang, 2023; Rubel & Jones, 2016).

The ethical implications of data privacy are further complicated by the commercial interests that often underpin online learning platforms. Zeide and Nissenbaum (2018) argue that many virtual education providers adopt marketplace norms that prioritize profit over educational values, thereby undermining the principles of democracy and equal access to education. This commodification of education raises critical questions about the ethical use of student data and the responsibilities of educational institutions to protect their learners' privacy. The shift towards a data-driven educational model necessitates a reevaluation of the ethical frameworks that govern data collection and usage, particularly in light of the potential for exploitation and misuse of sensitive information.

The issue of data security breaches is another critical aspect of privacy concerns in online learning. Cahyanto's (2023) literature review highlights the challenges associated with the dissemination of personal data, particularly in the context of educational technology. The potential for data breaches not only endangers individual privacy but also poses significant risks to the integrity of educational institutions. As cyber threats continue to evolve, it is essential for educational stakeholders to implement robust security measures to protect sensitive information from unauthorized access.

Furthermore, the concept of "privacy calculus," as discussed by Jiang et al. (2022), suggests that students weigh the perceived benefits of online learning against the risks to their privacy. This theoretical framework underscores the importance of trust in online learning environments; when students perceive a high risk of privacy violations, their willingness to engage with digital platforms diminishes. Educational institutions must therefore prioritize transparency and accountability in their data practices to foster a culture of trust among learners.

Institutional Policies and Accountability

The role of institutional policies in safeguarding student privacy is critical. Many educational institutions lack comprehensive privacy policies that address the specific challenges posed by online learning environments (Hasan, 2023; Marín et al., 2020). This gap can lead to inconsistent practices and a lack of accountability, leaving students vulnerable to privacy violations. Institutions must develop robust privacy frameworks that clearly outline data collection practices, consent mechanisms, and the rights of students regarding their personal information (Alier et al., 2021; Liu & Khalil, 2023). Additionally, training and awareness programs for educators and students can help foster a culture of privacy consciousness within online learning environments (Noh, 2014; Hasan, 2023).

In conclusion, the privacy concerns in online learning environments are multifaceted and require a nuanced understanding of the interplay between technology, ethics, and educational practices. As educational institutions continue to navigate the complexities of digital learning, it is imperative that they prioritize the protection of student privacy through robust policies, ethical

frameworks, and transparent data practices. By addressing these concerns, educational stakeholders can create a more secure and trustworthy online learning environment that fosters student engagement and success.

Perceptions of Students and Teachers

The increasing adoption of online learning platforms has brought privacy and data protection to the forefront of educational discourse. The perceptions of students and teachers regarding these issues are shaped by various factors, including technological advancements, ethical considerations, and institutional policies. As digital education continues to evolve, understanding these perceptions is essential for fostering trust, ensuring effective educational practices, and safeguarding personal data.

Student Perceptions of Privacy in Online Learning

Students often express significant concerns regarding privacy in online learning environments, particularly when learning analytics and data collection practices are involved. Research suggests that students' willingness to engage with digital platforms is directly influenced by their perceptions of data security. For instance, Mutimukwe et al. (2022) found that students who are apprehensive about privacy risks are less likely to participate in online educational activities, indicating that privacy concerns can inhibit engagement. Similarly, Kumi-Yeboah et al. (2023) reported that students, particularly from diverse backgrounds, often feel a loss of control over their personal data, which negatively impacts their learning experiences. Furthermore, Jiang et al. (2022) noted that students frequently perceive their privacy as compromised, with some reporting experiences of data leaks during online learning.

The "privacy calculus" theory, which describes the trade-off individuals make between perceived benefits and risks associated with sharing personal information, is highly relevant in online learning contexts. Research by Peng and Dutta (2022) indicates that when students perceive a high risk of privacy infringement, they are less likely to engage with digital platforms, despite recognizing the potential benefits of online education. Interestingly, Vu et al. (2020) found that while many students are aware of privacy risks, a subset of learners does not actively concern themselves with how their data is used, suggesting a complex relationship between awareness and concern.

Moreover, students' trust in educational institutions plays a crucial role in shaping their perceptions of privacy. When institutions implement transparent data protection policies, students are more likely to feel secure and engage with online learning environments (Jiang et al., 2022). Conversely, when privacy policies are ambiguous or poorly communicated, students may develop distrust, which can hinder their participation in digital education (Jiang et al., 2022).

Teacher Perceptions of Privacy and Data Security

Teachers also experience privacy concerns in online learning environments, though their perspectives differ from those of students. Educators are particularly concerned with safeguarding student data while ensuring accountability in digital classrooms. Research by

Wang and Heffernan (2010) emphasizes that educators must be aware of the specific types of personal information that students are hesitant to share, as privacy concerns can vary across disciplines. Additionally, Blackmon and Major (2023) highlight that many educators lack sufficient training on privacy issues related to technology-enhanced learning, leading to unintentional breaches of student privacy.

The shift to online learning, particularly during the COVID-19 pandemic, has exacerbated these concerns. Many teachers reported challenges in balancing the need for student engagement with privacy considerations, particularly when requiring students to use webcams and microphones for synchronous learning (Almekhled & Petrie, 2023). Research by Rajab and Soheib (2021) underscores that privacy concerns became especially pronounced during the pandemic, as students were increasingly required to use technologies that could infringe on their personal privacy.

Pre-service teachers also exhibit complex perceptions regarding privacy. While many advocate for robust data protection policies, there is often a disconnect between their awareness of these policies and their implementation in practice (Marín et al., 2022). Additionally, concerns about the adequacy of government regulations on data privacy in education contribute to uncertainty among educators, making it difficult for them to navigate the complexities of digital teaching (Marín et al., 2020).

Ethical and Technological Considerations in Data Protection

The ethical implications of data collection in online learning environments cannot be overlooked. The increasing use of learning analytics raises significant concerns regarding student privacy, particularly in relation to how data is collected, analyzed, and utilized (Liu & Khalil, 2023). Researchers emphasize that institutions must prioritize ethical considerations when implementing learning analytics to ensure that student privacy is respected (Hoel & Chen, 2016). Failure to address these concerns can lead to resistance from both students and educators, potentially undermining the legitimacy of digital learning platforms (Hoel & Chen, 2016).

Additionally, the commercialization of educational technologies has raised alarms about potential privacy violations. Şanal and Çiçek (2023) argue that the commodification of digital education can lead to uncontrolled privacy breaches, particularly when student data is collected and analyzed without explicit consent. The presence of commercial interests in online education introduces ethical dilemmas, as institutions must balance financial incentives with the responsibility to protect student data.

From a technological perspective, the security architecture of online learning platforms plays a crucial role in shaping perceptions of privacy. Romansky and Noninska (2016) highlight the importance of implementing robust authentication and encryption measures to prevent unauthorized access to student data. However, the rapid pace of technological advancements often outstrips the development of adequate privacy protections, leading to a gap between students' expectations and the reality of their experiences (Liu, 2024). This discrepancy can result in distrust and reluctance to fully engage with digital learning tools.

The Role of Institutional Policies in Privacy Protection

Institutional policies significantly influence how students and educators perceive privacy and data protection in online learning environments. Research by Tsai et al. (2020) underscores the importance of clear consent mechanisms in fostering student trust. When institutions establish transparent privacy policies that outline data collection practices, students are more likely to feel confident in engaging with online platforms. Similarly, Jones et al. (2021) found that faculty members share concerns about data collection practices, emphasizing the need for institutional policies that protect both students and educators. However, current privacy policies often lag behind technological advancements, creating vulnerabilities for both students and teachers (Marín et al., 2020). There is a pressing need for educational institutions to develop comprehensive data protection policies that are effectively communicated to all stakeholders. By fostering a culture of privacy awareness and accountability, institutions can enhance trust in online learning environments (Huang, 2023).

Artificial Intelligence and Privacy in Online Education

The integration of artificial intelligence (AI) in educational settings presents additional privacy challenges. AI-driven learning platforms rely on vast amounts of data to personalize educational experiences, raising concerns about data security and algorithmic bias (Huang, 2023). If not properly regulated, AI applications in education

Mitigating Privacy Risks in Online Learning: Strategies and Technologies

The rapid transition to online learning, particularly accelerated by the COVID-19 pandemic, has raised significant concerns regarding privacy risks associated with the use of educational technologies. Various strategies and technologies have been proposed or implemented to mitigate these risks, focusing on enhancing user control over personal data, ensuring compliance with privacy regulations, and fostering trust among users. This section synthesizes findings from multiple studies to provide a comprehensive overview of the current landscape of privacy protection in online learning environments.

One of the primary strategies for mitigating privacy risks in online learning is the customization of privacy settings by users. Research indicates that when platforms allow users to tailor their privacy preferences, it can significantly alleviate concerns regarding data exposure and misuse. Blackmon and Major (2023) highlight that students' concerns about privacy can be alleviated when platforms provide options for users to customize their privacy settings according to their preferences. This customization empowers learners by giving them agency over their personal information, thereby enhancing their overall trust in the educational platform. Trust is a crucial factor in the willingness to engage with online learning platforms, as Jiang et al. (2022) emphasize that learners' perceptions of data policies significantly influence their readiness to disclose sensitive information. Thus, platforms that prioritize user-friendly privacy settings can

effectively enhance user engagement and satisfaction.

Moreover, the implementation of robust data protection policies is crucial in addressing privacy concerns. Alier et al. (2021) argue that educational institutions must go beyond mere compliance with data protection regulations; they should actively engage in practices that prioritize the safeguarding of student data. While some solutions, such as data depersonalization, are often viewed as effective, they can be misleading, as depersonalized data can still be re-identified with minimal information. This underscores the necessity for educational institutions to adopt comprehensive data protection strategies that go beyond superficial measures. Transparent data handling practices, including encryption technologies and secure data storage, can significantly reduce the risk of data breaches and unauthorized access to personal information. Additionally, the establishment of clear data governance policies is vital to ensure that data collection and usage comply with legal and ethical standards. Reidenberg and Schaub (2018) advocate for accountability in the use of big data in education, emphasizing the need for stringent governance frameworks.

The use of learning analytics also presents both opportunities and challenges in the realm of privacy. While learning analytics can provide valuable insights into student performance and engagement, it raises ethical concerns regarding data privacy. Liu and Khalil (2023) argue that stakeholder perspectives on privacy and data protection in learning analytics are diverse and context-dependent, necessitating targeted research to understand these views before implementing analytics solutions. Implementing privacy-preserving techniques in learning analytics, such as differential privacy, can help mitigate risks while still allowing institutions to gain valuable insights from student data. This balance between data utility and privacy protection is crucial for the ethical use of learning analytics in education.

In addition to these strategies, the integration of privacy-enhancing technologies (PETs) is another effective measure to safeguard student data. Anwar (2020) discusses the importance of incorporating PETs in online learning systems to support privacy, trust, and personalization. These technologies can include encryption, anonymization, and secure data storage solutions that protect sensitive information from unauthorized access. By leveraging PETs, educational institutions can create a more secure online learning environment that prioritizes student privacy.

Furthermore, the ethical implications of artificial intelligence (AI) in education cannot be overlooked. Huang (2023) highlights the urgent need to address the ethical risks posed by AI technologies to student data privacy. As AI becomes increasingly integrated into educational platforms, it is essential to establish ethical guidelines that govern the use of AI in a manner that respects and protects student information. To address these challenges, it is imperative to develop AI systems that are transparent and accountable, ensuring that students are informed about how their data is being used. Moreover, educational institutions should engage in ongoing dialogue with stakeholders, including students, parents, and educators, to establish trust and transparency in AI applications. This collaborative approach can help mitigate concerns related to data

misuse and enhance the overall effectiveness of AI in educational settings.

The role of educators in safeguarding student privacy is also critical. Almekhled and Petrie (2023) note that teachers face challenges in monitoring student participation and engagement in online settings, which can inadvertently lead to privacy breaches. Educators must be trained to understand privacy risks and implement best practices in their online teaching methodologies. This includes being mindful of how they collect and use student data during assessments and interactions, thereby fostering a culture of privacy awareness within educational institutions. Moreover, Chang (2021) points out that many students are unaware of the privacy risks associated with online learning platforms, which can lead to unintentional data exposure. Therefore, implementing training programs that focus on digital literacy and data privacy awareness can empower users to make informed decisions regarding their online interactions. Such educational initiatives can foster a culture of privacy consciousness within educational institutions, encouraging users to take proactive measures to protect their personal information.

In the context of massive open online courses (MOOCs), Zeide and Nissenbaum (2018) emphasize the necessity for providers to go beyond compliance with data regulations and actively uphold student privacy norms. This involves not only adhering to legal requirements but also embracing ethical standards that prioritize the dignity and rights of learners. By fostering a culture of respect for privacy, MOOC providers can enhance the learning experience and encourage greater participation.

Additionally, the challenges posed by wearable technology in education further complicate privacy considerations. Cahyanto (2023) highlights that the use of such technologies can lead to significant privacy risks, particularly concerning the collection and dissemination of personal data. As educational institutions increasingly adopt wearable devices, it is imperative to implement stringent data protection measures that address these challenges and safeguard user privacy. Institutions should also consider implementing opt-in policies, allowing users to choose whether they want their data to be collected and used for educational purposes.

The ongoing discourse surrounding student data privacy in online learning environments underscores the need for continuous evaluation and improvement of privacy strategies. Almekhled and Petrie (2023) note that the experiences of educators during the pandemic have revealed persistent privacy and security issues that require ongoing attention. As technology continues to evolve, educational institutions must remain vigilant in assessing the effectiveness of their privacy measures and making necessary adjustments to address emerging risks. Chang's examination of student privacy issues in online learning environments highlights the evolving nature of these concerns and the necessity for adaptive solutions that respond to emerging threats (Chang, 2021).

In conclusion, the mitigation of privacy risks in online learning requires a multifaceted approach that encompasses user empowerment, robust data protection measures, ethical AI practices, user education, clear institutional policies, and continuous evaluation of privacy strategies. By adopting these strategies,

educational institutions can create secure online learning environments that prioritize student privacy and foster trust among users. As the landscape of online education continues to evolve, it is essential for stakeholders to remain engaged in discussions surrounding privacy and to implement best practices that protect the rights and data of learners.

Research Gaps and Suggestions for Future Research

In reviewing the literature on privacy in online learning, several critical gaps have been identified. Addressing these gaps is essential for developing a more comprehensive understanding of privacy concerns and ensuring that online learning environments are secure, inclusive, and effective for all users. The following areas require further research:

Lack of Focus on Specific Demographics

Many studies address privacy in online learning at a general level, but there is limited research on how privacy concerns vary across different demographics, including age, gender, cultural background, and socioeconomic status. Future research should explore privacy perceptions and practices among diverse learner populations and examine how cultural attitudes toward privacy influence engagement in online learning platforms.

Privacy in Emerging Learning Technologies

The rapid integration of artificial intelligence (AI), virtual reality (VR), and augmented reality (AR) in education has introduced new privacy challenges that remain understudied. Researchers should investigate the privacy implications of AI-driven tools, such as personalized learning systems, and assess how immersive technologies impact data collection and student privacy.

Longitudinal Studies on Privacy Impacts

Most existing research provides only cross-sectional insights into privacy concerns, leaving a gap in understanding how these issues evolve over time. Conducting longitudinal studies can help track changes in students' privacy awareness and behaviors throughout their educational journeys and evaluate the long-term effects of privacy breaches on trust in online learning systems.

Privacy by Design in Learning Management Systems (LMS)

While privacy frameworks exist, there is a lack of research on their implementation within popular LMS platforms. Future studies should assess how LMS platforms incorporate "privacy by design" principles, analyze the effectiveness of existing privacy settings, and propose improvements to enhance user privacy.

Intersection of Privacy and Accessibility

The interplay between privacy and accessibility for learners with disabilities remains underexplored. Further research is needed to investigate how privacy features impact accessibility for differently-abled learners and to develop frameworks that balance privacy protection with accessibility needs.

Privacy in Informal Online Learning Environments

Much of the existing research focuses on privacy concerns in formal learning platforms, neglecting informal environments such as

massive open online courses (MOOCs), social media, and community-based learning platforms. Future studies should examine privacy concerns specific to these contexts and analyze how platform policies protect user data in such informal settings.

Students' and Educators' Perspectives on Privacy

There is insufficient research comparing students' and educators' perceptions of privacy risks and needs. Comparative studies should be conducted to explore differences in privacy expectations and to assess how educators' privacy practices influence students' behaviors in online learning environments.

Regional and Policy Variations

Privacy concerns and regulations vary significantly across regions, yet comparative studies on their effectiveness are scarce. Future research should evaluate global privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Family Educational Rights and Privacy Act (FERPA) in the United States, to understand their impact on user trust and platform adoption.

Privacy and Data Transparency

Learners often lack awareness of how their data is collected, stored, and utilized by online learning platforms. Future research should investigate strategies to enhance transparency in data practices and assess the role of privacy literacy programs in empowering learners to make informed decisions about their online privacy.

Impact of Data Breaches on Learning Outcomes

The consequences of privacy breaches on student performance, participation, and trust in online learning systems remain under-researched. Future studies should examine the psychological and academic impacts of privacy violations and propose frameworks for rebuilding student trust following a data breach. By addressing these research gaps, future studies can contribute to a more comprehensive understanding of privacy in online learning and inform policies and practices that enhance user security and trust in digital education environments.

Discussion and Conclusion

The rapid expansion of online learning, accelerated by the COVID-19 pandemic, has brought unprecedented opportunities for education but also significant challenges related to privacy and data protection. This literature review has synthesized existing research to provide a comprehensive understanding of the multifaceted privacy concerns in online learning environments, including data collection, surveillance, ethical implications of learning analytics, and the role of institutional policies. The review also explored the perceptions of students and educators, highlighting the critical role of trust, transparency, and accountability in fostering secure and effective online learning experiences.

Key findings reveal that privacy concerns in online learning are pervasive and complex, influenced by technological advancements, ethical considerations, and institutional practices. Students and educators alike express apprehension about data security, unauthorized

access, and the misuse of personal information, which can hinder engagement and trust in digital platforms. The integration of emerging technologies such as artificial intelligence (AI), virtual reality (VR), and augmented reality (AR) further complicates these issues, introducing new privacy risks that require careful consideration.

To mitigate these risks, the review identified several strategies and technologies, including customizable privacy settings, robust data protection policies, privacy-enhancing technologies (PETs), and ethical AI practices. However, the effectiveness of these measures depends on their implementation and the extent to which they are communicated to and understood by users. Institutional policies play a crucial role in safeguarding privacy, yet many educational institutions lack comprehensive frameworks that address the unique challenges of online learning.

The review also highlighted significant gaps in the literature, including the need for research on specific demographics, the privacy implications of emerging technologies, longitudinal studies, and the intersection of privacy and accessibility. Additionally, there is a pressing need for comparative studies on regional privacy regulations and their impact on user trust, as well as research on the psychological and academic consequences of data breaches.

In conclusion, as online learning continues to evolve, it is imperative for educational institutions, policymakers, and technology providers to prioritize privacy and data protection. By addressing the identified gaps and implementing best practices, stakeholders can create secure, inclusive, and trustworthy online learning environments that empower learners and educators alike. Future research should focus on developing adaptive solutions that respond to emerging privacy challenges, ensuring that the benefits of digital education are realized without compromising the rights and security of users.

Funding: This research did not receive a specific grant from public, commercial, or not-for-profit funding agencies.

Declaration of Competing Interest: The authors declare no competing interests.

References

Alier, M., Guerrero, M., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and e-learning: A pending task. *Sustainability, 13*(16), Article 9206. https://doi.org/10.3390/su13169206

Almekhled, B., & Petrie, H. (2023). Privacy and security in online teaching during the COVID-19 pandemic: Experiences and concerns of teachers in UK higher education. *British Journal of Educational Technology.* https://doi.org/10.14236/ewic/bcshci2023.24

Anwar, M. (2020). Supporting privacy, trust, and personalization in online learning. *International Journal of Artificial Intelligence in Education, 31*(4), 769–783. https://doi.org/10.1007/s40593-020-00216-0

Blackmon, S., & Major, C. (2023). Inclusion or infringement? A systematic research review of students' perspectives on student privacy in technology-enhanced, hybrid and online courses. *British Journal of Educational Technology, 54*(6), 1542–1565. https://doi.org/10.1111/bjet.13362

Cahyanto, I. (2023). Privacy challenges in using wearable technology in education: Literature review. *Formosa Journal of Applied Sciences, 2*(6), 909–928. https://doi.org/10.55927/fjas.v2i6.4272

Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education, 42*(1), 55–69. https://doi.org/10.1080/01587919.2020.1869527

Fernando, W., Mel, W., Rajapakse, N., & Kumara, I. (2022). Impact of online learning readiness on online learning effectiveness. *World Journal of Advanced Research and Reviews, 16*(3), 627–633. https://doi.org/10.30574/wjarr.2022.16.3.1364

Hasan, R. (2023). Understanding EdTech's privacy and security issues: Understanding the perception and awareness of educational technologies' privacy and security issues. *Proceedings on Privacy Enhancing Technologies, 2023*(4), 269–286. https://doi.org/10.56553/popets-2023-0110

He, L. (2022). Pathways to social presence in online learning communities. *Learning & Education, 10*(8), 91. https://doi.org/10.18282/l-e.v10i8.3070

Hoel, T., & Chen, W. (2016). Privacy-driven design of learning analytics applications: Exploring the design space of solutions for data sharing and interoperability. *Journal of Learning Analytics, 3*(1), Article 9. https://doi.org/10.18608/jla.2016.31.9

Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers, 16*(2), 2577–2587. https://doi.org/10.15354/sief.23.re202

Jiang, X., Goh, T., & Liu, M. (2022). On students' willingness to use online learning: A privacy calculus theory approach. *Frontiers in Psychology, 13*, Article 880261. https://doi.org/10.3389/fpsyg.2022.880261

Jones, K., VanScoy, A., Bright, K., & Harding, A. (2021). Do they even care? Measuring instructor value of student privacy in the context of learning analytics. *Hawaii International Conference on System Sciences*, Article 185. https://doi.org/10.24251/hicss.2021.185

Karuniawan, A. (2023). Bibliometric analysis of online learning in the era of technological progress. *Jentik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 2*(2), 48–53. https://doi.org/10.58723/jentik.v2i2.227

Kumi-Yeboah, A., Kim, Y., Yankson, B., Aikins, S., & Dadson, Y. (2023). Diverse students' perspectives on privacy and technology integration in higher education. *British Journal of Educational Technology, 54*(6), 1671–1692. https://doi.org/10.1111/bjet.13386

Liu, M. (2024). Instructors' usage of mobile learning applications in classroom and its impact on the learners' performance. *World Journal of Educational Research, 11*(1), 48–58. https://doi.org/10.22158/wjer.v11n1p48

Liu, Q., & Khalil, M. (2023). Understanding privacy and data protection issues in learning analytics using a systematic review. *British Journal of Educational Technology, 54*(6), 1715–1747. https://doi.org/10.1111/bjet.13388

Ma, Y., Xiang, S., & Yang, H. (2023). Research on the effect of learner characteristics on postgraduate online learning. *Proceedings of the 2023 International Conference on Education and Artificial Intelligence*, 1099–1103. https://doi.org/10.2991/978-94-6463-192-0_143

Marín, V., Carpenter, J., & Tur, G. (2020). Pre-service teachers' perceptions of social media data privacy policies. *British Journal of Educational Technology, 52*(2), 519–535. https://doi.org/10.1111/bjet.13035

Marín, V., Carpenter, J., Tur, G., & Williamson-Leadley, S. (2022). Social media and data privacy in education: An international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education, 10*(4), 769–795. https://doi.org/10.1007/s40692-022-00243-x

Mawene, E. (2023). Benefits of online learning for students of the PPKn study program class of 2020 during the COVID-19 pandemic. *Jurnal*

Pendidikan Amartha, 2(1), 55–61. https://doi.org/10.57235/jpa.v2i1.428

Mutimukwe, C., Viberg, O., Oberg, L. M., & Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology, 53*(4), 932–951. https://doi.org/10.1111/bjet.13234

Noh, Y. (2014). Digital library user privacy: Changing librarian viewpoints through education. *Library Hi Tech, 32*(2), 300–317. https://doi.org/10.1108/lht-08-2013-0103

Orikana, M., Yulia, H., & Krismiyati, K. (2022). Effectiveness of online learning viewed from students' online interaction. *Jurnal Teknologi Informasi dan Pendidikan, 15*(1), 105–119. https://doi.org/10.24036/jtip.v15i1.576

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology, 45*(3), 438–450. https://doi.org/10.1111/bjet.12152

Peng, M., & Dutta, B. (2022). Impact of personality traits and information privacy concern on e-learning environment adoption during the COVID-19 pandemic: An empirical investigation. *Sustainability, 14*(13), Article 8031. https://doi.org/10.3390/su14138031

Rajab, M., & Soheib, M. (2021). Privacy concerns over the use of webcams in online medical education during the COVID-19 pandemic. *Cureus.* https://doi.org/10.7759/cureus.13536

Reidenberg, J., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education, 16*(3), 263–279. https://doi.org/10.1177/1477878518805308

Romansky, R., & Noninska, I. (2016). Architecture of combined e-learning environment and investigation of secure access and privacy protection. *International Journal of Human Capital and Information Technology Professionals, 7*(3), 89–106. https://doi.org/10.4018/ijhcitp.2016070107

Rubel, A., & Jones, K. (2016). Student privacy in learning analytics: An information ethics perspective. *The Information Society, 32*(2), 143–159. https://doi.org/10.1080/01972243.2016.1130502

Şanal, S., & Çiçek, B. (2023). University students' digital spaces in online learning communities: Implications for understanding, protecting and maintaining privacy. *British Journal of Educational Technology, 55*(2), 654–667. https://doi.org/10.1111/bjet.13390

Santoso, H., Riyanti, R., Prastati, T., S., F., Susanty, A., & Yang, M. (2022). Learners' online self-regulated learning skills in Indonesia Open University: Implications for policies and practice. *Education Sciences, 12*(7), Article 469. https://doi.org/10.3390/educsci12070469

Sasmita, N., Redhana, I., & Suja, I. (2021). The effect of online learning on students' learning achievement on colloid concept. *Proceedings of the Annual International Conference on Education and e-Learning.* https://doi.org/10.2991/assehr.k.210312.059

Syarbini, N., Maulana, A., & Arif, W. (2022). Analysis of online learning motivation in students XI SMA Negeri 1 Jeneponto. *Journal of Islam and Science, 9*(2), 94–98. https://doi.org/10.24252/jis.v9i2.31119

Tsai, Y., Whitelock-Wainwright, A., & Gašević, D. (2020). The privacy paradox and its implications for learning analytics. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 230–239). https://doi.org/10.1145/3375462.3375536

Vu, P., Adkins, M., & Henderson, S. (2020). Aware, but don't really care: Students' perspective on privacy and data collection in online courses. *The Journal of Open, Flexible and Distance Learning, 23*(2), 42–51. https://doi.org/10.61468/jofdl.v23i2.350

Wang, R., Han, J., Liu, C., & Wang, L. (2022). Relationship between medical students' perceived instructor role and their approaches to using online learning technologies in a cloud-based virtual classroom. *Research Square.* https://doi.org/10.21203/rs.3.rs-1406388/v2

Wang, S., & Heffernan, N. (2010). Ethical issues in computer-assisted language learning: Perceptions of teachers and learners. *British Journal of Educational Technology, 41*(5), 796–813. https://doi.org/10.1111/j.1467-8535.2009.00983.x

Zeide, E., & Nissenbaum, H. (2018). Learner privacy in MOOCs and virtual education. *Theory and Research in Education, 16*(3), 280–307. https://doi.org/10.1177/1477878518815340