Privacy by Design in AI-Enhanced Education: Navigating U.S. Legal Requirements and Ethical Design Practices

Oluwatayo Osodein [1*], Ayomide Arowolo Ayodeji [2], Oluwatimileyin Osodein [3], Owoeye Temitope [4], Cletus Oladimeji [5], Durotoye Kolapo Ibidoja [6], Sam Anibe Peter [7]
[1-7] Kogi State University, Nigeria

* Corresponding Author: **Oluwatayo Osodein**

Article Info

P-ISSN: 3051-3502
E-ISSN: 3051-3510
Volume: 07
Issue: 01
Received: 16-01-2026
Accepted: 18-02-2026
Published: 20-03-2026
Page No: 107-123

Abstract
In order to close significant gaps in the privacy protection of student data in educational AI systems, this study looked at how Privacy by Design principles are incorporated into AI-enhanced educational technologies and how well they match US legal requirements. This research shows notable differences in privacy implementation and legal compliance by conducting a systematic analysis of privacy practices across popular educational AI platforms, such as Khan Academy, Coursera, and commercial learning management systems. The results show that although 77% of platforms do not make privacy a default setting, Khan Academy is a prime example of how strong privacy safeguards and effective education can coexist, as evidenced by its high user satisfaction ratings and extensive data protection policies. According to the analysis, there are ongoing issues with consent protocols, with 67% of platforms gathering behavioral data beyond what is required for education, and there are extensive shortcomings in transparency procedures that make privacy policies unintelligible to important stakeholders. Strong correlations between the implementation of privacy features and user satisfaction are confirmed by statistical analysis ($r=0.73$, $p<0.001$), which defies industry presumptions regarding trade-offs between privacy and functionality. Critical ethical blind spots in current implementations are identified by the research, such as the systematic exclusion of student voices from privacy design decisions and the failure to adequately consider the long-term implications of educational data profiling. These results demonstrate the pressing need for institutional commitment to Privacy by Design principles, improved regulatory enforcement, and coordinated policy reform. The study offers practical suggestions for enhancing privacy practices in educational AI systems that benefit millions of students across the country, while also adding empirical support to theoretical frameworks.

DOI: https://doi.org/10.54660/IJMER.2026.7.1.107-123

Keywords: Privacy by Design, Educational Artificial Intelligence, Student Data Protection, FERPA Compliance, Educational Technology Ethics

Introduction

The integration of artificial intelligence and adaptive learning technologies in educational environments has radically altered the environment of education, bringing a new era of data-heavy and customized education. An example of such transformation can be seen in AI-enhanced educational platforms - systems that apply artificial intelligence to different extents in the context of the wider educational technology system. Examples of these on either side of the AI integration spectrum include Khan Academy (which uses the Khanmigo AI-driven tutoring in addition to conventional teaching content), Coursera (which uses AI to make personalized recommendations to students and provide support), Pearson's MyLab (which uses adaptive learning algorithms to score and provide feedback), and MATHia (which uses AI to personalize mathematics learning content).

These platforms accumulate considerable information regarding the learning process, preferences, behavioral patterns, and performance measures of the students, but they differ in the extent to which AI will lead to the core educational processes, as compared to the performance of the human-created content. It should be mentioned that this research looks into AI-enhanced educational platforms, which can be explained as the educational technology systems which have the ability to support, supplement, or personalise the learning experiences by integrating AI capabilities, and not necessarily fully AI-generated or AI-driven educational systems. Such an inclusive definition indicates the present state of educational technology, where integration of AI lies on a spectrum between auxiliary applications (e.g. AI-powered tutoring assistants in largely traditional platforms) and more full-blown AI-based adaptive systems. Privacy concerns that were discussed in this paper apply to the entire range of the spectrum since regardless of whether AI technologies are incorporated into education or not, issues of data collection, data processing and data security are the concern when AI technologies are involved in a learning process, no matter how self-sufficient the AI technologies are in terms of content delivery.

Across the United States, classrooms from elementary schools to universities are now equipped with AI-enhanced education systems, which include automated assessment tools, adaptive learning platforms, predictive analytics dashboards, and intelligent tutoring systems (Baker & Smith, 2019) [2]. With the ability to identify at-risk students before they fall behind, provide individualized learning experiences catered to each student's needs, and optimize instructional strategies through real-time data analysis, these advanced technologies have the potential to completely transform education (Zawacki-Richter *et al*., 2019). The spread of AI tutoring programs is a prime example of this change in education, as sites such as Pearson's MyLab and Carnegie Learning's MATHia gather a great deal of detailed information about student interactions, learning styles, and cognitive processes (Holstein *et al*., 2018). In order to modify the content difficulty and presentation in real-time, adaptive learning technologies further complicate this data collection by continuously tracking student responses, engagement metrics, time-on-task measurements, and behavioral patterns (Siemens & Long, 2011). To generate thorough student profiles that guide institutional decision-making, educational analytics systems combine this data with demographic information, academic records, and even biometric indicators (Ferguson, 2012) [11].

These AI-enhanced educational systems' vast data collection capabilities, however, have raised serious privacy issues and ethical questions that could jeopardize the very educational advantages they are meant to offer. Concern over the surveillance-like tracking of learning behaviors, the possibility of algorithmic bias in educational recommendations, and the long-term effects of keeping comprehensive digital profiles of kids and teens are growing among students, parents, educators, and privacy advocates (Singer & Hill, 2020). Significant concerns regarding consent, data ownership, and the proper limits of educational surveillance are brought up by the sensitive nature of educational data, which frequently includes behavioral indicators, social interactions, psychological tests, and academic performance metrics (Reidenberg & Schaub, 2018). The involvement of several stakeholders with different responsibilities and interests adds to the complexity of these privacy issues. While technology companies look to expand their markets and monetize data, educational institutions aim to use AI technologies to enhance learning outcomes and operational efficiency (Williamson, 2017). Families and students want individualized education, but they might not fully comprehend the privacy implications of having their data gathered, examined, and possibly shared with outside parties (Hoofnagle *et al*., 2010). This complex ecosystem produces conflicts between privacy protection and innovative education that need to be carefully managed using both technical and legislative solutions.

As a result of these growing worries, the idea of Privacy by Design (PbD), first introduced by Ann Cavoukian in 2009, has become a crucial framework for dealing with privacy issues in educational systems that use artificial intelligence. A paradigm shift from reactive privacy protection measures to proactive integration of privacy considerations throughout the entire system development lifecycle is represented by Privacy by Design (Cavoukian, 2011) [7]. A thorough method for creating privacy-preserving educational technologies is offered by the framework's seven guiding principles: proactive rather than reactive, privacy as the default setting, full functionality, end-to-end security, visibility and transparency, respect for user privacy, and privacy embedded into design (Cavoukian, 2009) [6]. The way educational AI systems gather, process, store, and distribute student data must be fundamentally rethought in order to apply Privacy by Design principles. PbD requires that privacy protection be integrated into the fundamental design and operation of educational AI systems from the outset, rather than being treated as an afterthought or compliance requirement (Rubinstein & Good, 2020). To maintain educational efficacy while protecting student privacy, this strategy calls on educational technology developers to employ strategies like data minimization, purpose limitation, differential privacy, and federated learning (Dwork, 2008; McMahan *et al*., 2017) [8].

The legal environment in the US pertaining to educational privacy is complicated, with both federal and state laws having a big influence on how AI-enhanced educational systems are developed and implemented. Enacted in 1974 and later amended, the Family Educational Rights and Privacy Act (FERPA) gives parents and eligible students specific rights regarding access to and disclosure of educational information, as well as fundamental protections for student educational records (U.S. Department of Education, 2011). Additional protections for children under 13 are provided by the Children's Online Privacy Protection Act (COPPA), which mandates verifiable parental consent before collecting personal data from young children online (Federal Trade Commission, 2013) [10]. States like California have implemented comprehensive privacy laws like the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which extend privacy protections to educational contexts. This regulatory environment is further complicated by state-level legislation (California Attorney General, 2020) [5]. Furthermore, new state laws that target student data privacy specifically, like those passed in Connecticut, Illinois, and New York, place additional requirements on educational technology providers and result in a patchwork of compliance obligations that differ greatly between jurisdictions (Student Data Privacy Consortium, 2019).

For educational institutions and technology providers, the combination of these legal requirements with the technical capabilities and limitations of AI systems presents special difficulties. There are ambiguities in interpretation and application that necessitate careful legal and technical analysis because traditional privacy laws were not created to handle the complex data processing capabilities of contemporary AI systems (Solove, 2021). Conventional ideas of data processing purposes and consent mechanisms established in current privacy legislation are challenged by the dynamic nature of AI systems, which constantly learn and adapt based on new data (Wachter & Mittelstadt, 2019). This study is important because it has the potential to close the gap between the actual implementation of privacy-preserving AI systems in educational settings and the requirements of legal compliance. Clarity on how to manage privacy regulations while preserving educational efficacy is crucial as educational institutions depend more and more on AI technologies to improve learning outcomes and operational efficiency (Pardo & Siemens, 2014). By investigating how Privacy by Design principles can be operationalized within the limitations of U.S. educational privacy laws while maintaining the pedagogical benefits of AI-enhanced learning systems, this study fills a critical knowledge gap.

Nevertheless, this study also adds to the larger conversation about responsible AI development by showing how privacy-preserving design principles can be effectively incorporated into domain-specific applications. Because of the vulnerability of student populations, the long-term effects of collecting educational data, and the public interest in making sure that technological innovation promotes rather than jeopardizes educational equity and student welfare, the educational sector makes an especially compelling case study (Zeide, 2017). This research attempts to guide institutional decision-making, inform policy development, and advance industry best practices that put student privacy protection and educational innovation first by creating frameworks and recommendations for privacy-preserving AI in education.

Statement of the Problem

There is a significant gap between the rate of technological advancement and the adoption of sufficient privacy protections that preserve student data and guarantee adherence to changing legal and ethical norms, even in spite of the quick spread of artificial intelligence technologies in educational settings. The current state of AI-enhanced educational tools reveals a concerning trend: advanced data collection and processing capabilities are used without giving enough thought to privacy implications, resulting in settings where students' personal data, learning habits, and cognitive patterns are widely tracked and analyzed with little to no transparency or meaningful consent mechanisms.This technological development has surpassed the creation of comprehensive privacy protection frameworks tailored to educational AI systems, leading to a disjointed approach to student data protection that ignores the particular vulnerabilities present in educational settings where students and institutions hold power imbalances, sensitive academic and developmental data, and the long-term effects of digital profiling. Furthermore, because educational institutions and technology vendors find it difficult to operationalize privacy-preserving design principles while preserving the functionality and efficacy of their AI tools, there is a stark disconnect between the theoretical underpinnings of Privacy by Design and their actual application within AI-enhanced educational systems.

Many educational technology providers find it difficult to effectively navigate the complex web of compliance requirements created by the intersection of emerging state-level privacy legislation with federal laws like FERPA and COPPA. This makes the challenge even more complicated. With their frequent adoption of privacy practices that may technically adhere to current laws but fall short of the proactive, all-encompassing approach to privacy protection envisioned by Privacy by Design principles, current AI educational tools operate within this regulatory uncertainty, exposing educational institutions to legal and reputational risks as well as students to privacy violations. Given that the lack of systematic assessment of privacy practices in educational AI has created a knowledge gap that hinders stakeholders from understanding the true extent of privacy risks and the effectiveness of current protection measures, as well as the development of evidence-based recommendations for improving privacy practices in this crucial sector that affects millions of students nationwide, there is an urgent need for an empirical examination of how current AI-enhanced educational systems align with both Privacy by Design principles and current U.S. legal requirements.

Research Questions

This research attempts to offer thorough responses to basic concerns regarding privacy protection in AI-enhanced learning environments in order to close these significant knowledge and practice gaps. This investigation of the state of privacy practices today and the possibility of better protection mechanisms in educational AI systems is guided by the following research questions.

1. How much do AI-enhanced educational technologies utilized in American institutions incorporate privacy by design principles?
2. In what ways do these technologies comply with current US legal requirements, such as COPPA and FERPA?
3. What ethical issues arise when educators and developers incorporate privacy features?
4. How can AI be used in education in a way that is more ethically and legally acceptable?

Literature Review/Theoretical Underpinnings

A rapidly growing body of literature has emerged from the nexus of artificial intelligence and educational technology, highlighting the transformative potential as well as the serious privacy issues that arise in AI-enhanced learning environments. Learning analytics systems that process large amounts of student behavioral data to predict academic outcomes, adaptive learning platforms that dynamically adjust content difficulty and presentation methods, intelligent tutoring systems that provide personalized instruction based on individual learning patterns, and automated assessment tools that assess student performance across multiple dimensions are just a few examples of the diverse array of technologies that make up modern educational AI systems (Zawacki-Richter *et al.*, 2019).

Through the creation of data-rich environments where every student interaction—from mouse clicks to time spent reading particular content—becomes a data point for algorithmic analysis and decision-making, these technologies radically transform the conventional educational paradigm (Williamson, 2017). Technological developments in machine

learning, natural language processing, and educational data mining have sped up the spread of these systems, allowing for previously unheard-of levels of automation and personalization in the delivery of education (Baker & Inventado, 2014) [1].

The creation of thorough privacy protection frameworks tailored for educational settings has lagged behind this technological revolution, though, leaving a big gap between innovation and responsible application. Since students frequently have little control over system adoption and little knowledge of the implications of data collection, the educational technology sector has largely adopted privacy practices designed for general consumer applications, failing to take into account the unique vulnerabilities and power dynamics present in educational settings (Reidenberg & Schaub, 2018). According to research by Singer and Isaac (2016), a large number of educational technology companies use commercial data sharing agreements that commodify student information, psychological profiling, behavioral monitoring, and other extensive data collection methods that go well beyond educational necessity. This trend has raised serious concerns among educators, legislators, and privacy advocates who contend that the current practices violate basic student privacy principles and pose long-term risks to educational equity and learner autonomy (Zeide, 2017). A theoretical framework for tackling these privacy issues through the proactive integration of privacy protections throughout the technology development lifecycle is provided by the Privacy by Design concept, which was first introduced by Ann Cavoukian in 2009.

According to Cavoukian's seven foundational principles, privacy protection should be proactive rather than reactive, implemented as the default setting rather than an optional feature, designed to preserve full system functionality without compromising privacy, secured by end-to-end protection mechanisms, operated with complete transparency and visibility, and respected for user privacy throughout all interactions. Additionally, it should be integrated into the core system design rather than added as an afterthought (Cavoukian, 2011) [7]. The General Data Protection Regulation (GDPR) of the European Union, which requires privacy by design and by default for all data processing activities, is one of the significant privacy regulations that incorporates these principles, which have gained international recognition (Rubinstein & Good, 2020).

Sophisticated technical strategies that strike a balance between privacy protection and educational efficacy are needed to apply Privacy by Design principles to educational AI systems. Differential privacy research by Dwork and Roth (2014) [9] has shown how mathematical methods can allow for statistical analysis of educational data while offering formal privacy guarantees for specific students. According to McMahan *et al*. (2017), federated learning techniques present viable ways to train AI models on dispersed educational data without centralizing private student data. The majority of commercial educational AI systems still rely on centralized data collection and processing models that maximize data utility at the expense of student privacy, indicating that the practical application of these privacy-preserving technologies in educational contexts is still limited (Holstein *et al*., 2018).

The intricate web of federal and state laws pertaining to educational privacy in the United States has a big influence on how AI-enhanced educational systems are developed and implemented. Parents and eligible students have the right to access, review, and control the disclosure of educational information thanks to the Family Educational Rights and Privacy Act (FERPA), which was passed in 1974 and has since undergone numerous amendments. FERPA provides the fundamental privacy protections for student educational records (U.S. Department of Education, 2011). But there is still uncertainty about how FERPA applies to contemporary AI systems, especially when it comes to whether behavioral data, learning analytics, and algorithmic inferences qualify as educational records that are protected by statute (Reidenberg *et al*., 2013). According to the Federal Trade Commission (2013) [10], educational AI vendors take advantage of the substantial gaps created by the Children's Online Privacy Protection Act (COPPA), which requires verifiable parental consent for online data collection and offers additional protections for children under the age of 13. With California spearheading the creation of comprehensive privacy frameworks through the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), which extend significant privacy rights to educational contexts, state-level privacy legislation has emerged as a crucial supplement to federal protections (California Attorney General, 2020) [5].

Educational technology providers are subject to additional requirements, such as data minimization obligations, purpose limitations, and enhanced parental notification requirements, by student-specific privacy laws, such as Illinois' Student Online Personal Protection Act and New York's Education Law Section 2-d (Student Data Privacy Consortium, 2019). But for educational AI vendors that operate in several jurisdictions, this patchwork of state and federal laws makes compliance difficult, frequently leading to the use of lowest-common-denominator approaches to privacy protection that fall short of offering sufficient protections (Purtova, 2018).

Beyond merely adhering to the law, ethical design frameworks have become crucial theoretical tools for assessing the moral implications of educational AI systems. Value Sensitive Design (VSD) is a methodical approach to technology design that takes human values into consideration at every stage of development. Designs are assessed for their effects on values like justice, dignity, and privacy in addition to their usability and functionality (Friedman *et al*., 2013) [12]. With regard to educational technology in particular, VSD provides a framework for resolving issues of value alignment between technological capabilities and learning objectives, taking into account the values of individual stakeholders as well as larger cultural contexts (Viberg *et al*., 223). Several stakeholder perspectives, including those of students, teachers, parents, administrators, and society at large, must be carefully taken into account when applying VSD to educational AI. These stakeholders may have differing views on privacy, autonomy, transparency, and the efficacy of education (Umbrello, 2019).

Another theoretical lens for analyzing the ethical aspects of educational AI design is responsible innovation theory, which highlights the necessity of reflexivity, adaptive management, anticipatory governance, and stakeholder inclusion throughout the innovation process (Stilgoe *et al*., 2013). Because it acknowledges that privacy harms might not be evident until years after initial deployment, when students have graduated and entered professional contexts where their educational data profiles may influence opportunities and outcomes, this framework is especially pertinent to

educational AI (Owen *et al*., 2012). According to Blok and Lemmens (2015) [3], the theory's emphasis on reflexivity necessitates constant evaluation of the effects of innovation and modification of development practices in response to new evidence of harm or benefit. This is especially crucial in light of the rapidly advancing capabilities of AI and the possibility of unforeseen consequences in educational settings. Even with the theoretical underpinnings offered by VSD, Responsible Innovation Theory, and Privacy by Design, there are still a lot of unanswered questions about empirical research relating AI design practices to moral and legal compliance in educational settings. The majority of current research concentrates on technical privacy-preserving techniques without analyzing how well they work in real-world commercial educational AI systems or how well they satisfy regulatory requirements (Prinsloo & Slade, 2017).

According to research by Tsai *et al*. (2020), parents and educators frequently find educational technology privacy policies to be unintelligible, which raises concerns about meaningful consent and transparency in data collection practices. Likewise, research by Hoel and Chen (2016) [13] and Bulger *et al*. (2017) [4] found notable discrepancies between declared privacy safeguards and real data handling procedures in the use of educational technology. By going beyond conventional tort law ideas to address the complex terrain of information privacy violations in digital environments, Solove's Taxonomy of Privacy offers a thorough framework for comprehending the particular kinds of privacy harms that may result from AI-enhanced educational systems (Solove, 2006). The taxonomy divides privacy harms into four main categories: invasion (intrusion and decisional interference), information processing (aggregation, identification, secondary use, insecurity, and exclusion), information dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion), and information collection (surveillance and interrogation). This framework is especially pertinent to educational AI systems, which collect a lot of data through behavioral monitoring, process complex data through algorithmic analysis and profiling, potentially disseminate information through data sharing agreements, and intrude through automated decision-making that impacts student opportunities and results.

A thorough basis for assessing privacy practices in AI-enhanced educational systems is provided by the integration of these theoretical frameworks. Responsible Innovation Theory tackles governance and stakeholder engagement; VSD offers a values-based approach to design evaluation; Privacy by Design offers technical and procedural principles for implementation; and Solove's Taxonomy makes it possible to systematically identify and classify privacy harms. These frameworks work together to provide a comprehensive evaluation of how educational AI systems strike a balance between technological functionality and human values, innovation and privacy protection, and ethical obligations. Through a methodical assessment of privacy practices in implemented educational technologies, this study seeks to fill a critical research gap: the empirical application of these frameworks to real educational AI systems.

Methodology

The present study incorporated a convergent parallel mixed-methods research design, which combined quantitative and qualitative data to give a detailed analysis of the privacy practices in AI-enhanced educational systems. The process of data collection and analysis was performed simultaneously in September 2024 to January 2025, with the same emphasis on the two strands of methodology.

Research Scope and Platforms

The research used five popular AI-enhanced education websites, i.e., Khan Academy, Coursera, Pearson, MyLab, and Mastering, ALEKS provided by McGraw-Hill, and DreamBox Learning. It is possible to choose these platforms because they are widely used in K-12 and higher education settings and are based on learner data to be personalized and analyzed.

Data Collection Methods

1. **Document Analysis:** Systematic document analysis of publicly available documents of each platform was performed, i.e., privacy policies, terms of service, data processing agreements, technical documentation, and design specifications. The analysis reviewed how each platform implemented the Privacy by Design principles, adhered to the existing privacy laws that govern the U.S. (FERPA, COPPA and state laws), and described clear data management policies. Results of this element were used in the comparative evaluation of platform privacy architecture.
2. **Online Survey:** The quantitative data were gathered using a structured online survey which was administered via professional educational technology networks, institutional contacts and through pertinent associations (e.g., ISTE, CoSN and regional educational technology consortia). The survey focused on teachers, administrators, and IT specialists who are directly introduced to the chosen platforms. The tool used a five-point Likert-scale question describing privacy knowledge, experience of implementation, perceived sufficiency of privacy controls, and user satisfaction. Out of 200 surveys sent out between October and November 2024, 187 valid returns were achieved and the response rate was 93.5%.
3. **Semi-Structured Interviews:** Semi-structured interviews with 15 purposely selected participants, who represented three groups of stakeholders, (a) Platform developers and privacy officers (b) School district administrators and Chief Technology Officers (c) Legal experts in the field of educational privacy law, yielded qualitative information. The sample was recruited using professional networks, direct approach to platform providers and recommendations by educational technology associations. All interviews reasons were done online, using video conferencing, during November 2024 to January 2025 and of 45-60 minutes. The interview questions were aimed at the issues of implementation of privacy, regulatory compliance, ethical aspects, and suggestions to enhance privacy protection in educational AI systems.

Data Analysis Procedures

The data obtained in the quantitative survey was processed on SPSS (version 25) through the application of descriptive and inferential statistics to determine the trends in privacy awareness, perceptions, and satisfaction. Thematic analysis through NVivo was used to analyze qualitative data of interviews and document analysis that enabled the

identification of recurring themes of privacy implementation, compliance issues, and ethical issues.

Integration of Findings

The quantitative and qualitative analyses were combined by developing a comparative evaluation matrix that evaluated the privacy practices of each platform in relation to the seven Privacy by Design principles and applicable legal standards. This integrative analysis allowed identifying the best practices, areas of compliance, and areas that need to be improved in existing AI-driven educational platforms.

Data Source Clarification

In order to be transparent in reporting, all sources of data are specified:

1. **Document Analysis:** Source contains privacy policy features, Privacy by Design compliance ratings, and legal compliance ratings (Tables 3, 4, and 7).
2. **Online Survey (Field Survey, 2025):** Source of the quantitative results of Tables 5, 6, and 9-16.
3. **Semi-Structured Interviews (Interview Analysis):** Thematic Findings and Qualitative Analysis (Table 8).
4. Tables that are labeled by SPSS 25 represent statistical analyses by using SPSS statistical software version 25.

Ethical Concerns and Research Compliance.

This study was carried out based on the standards of ethical research when dealing with human subjects. Informed consent was given to all the participants prior to either taking part in the surveys or interviews. In the case of survey participants, the informed consent was taken in the form of a digital consent form that was given at the start of the online questionnaire. The consent form provided information on the purpose of the study, suggest procedures, risks and benefits, and protection of confidentiality, voluntary nature of participation and right to withdraw. The respondents had to actively express their agreement prior to viewing survey questions. No personally identifiable data was stored and survey data were considered anonymous.

In the case of the interview participants, informed consent was achieved in two phases. To begin with, potential subjects were provided with comprehensive written information about the study, through email, including the consent form to read. Second, verbal consent was acquired and documented at the start of every video-taped interview, and the participants clearly stated that they understood and agreed to take part. The participants of the interview were assured that their answers will be de-identified in research publications and that the information identifying them will not be kept together with the interview data but will be kept in separate files which will be secured with a password.

Regarding the platforms analyzed in this study, it is necessary to explain that the document analysis aspect implied the analysis of publicly available resources (privacy policies, terms of service, technical documentation) that do not qualify as human subjects research according to the federal regulation (45 CFR 46). None of the user data of these platforms was accessed, and there were no participants in the research who were direct platform users. The participants of survey and interview were people (educators, administrators, technology specialists, and legal professionals) who presented their professional understanding of educational technology privacy practices; they were not required to disclose confidential platform information and breach terms of service.

Every data was managed according to the relevant data protection laws. The responses of the survey were stored in secure servers where the transmission was encrypted. The content of the transcripts and interview recordings were stored in encrypted devices with passwords that can only be accessed by the research team. Anonymized information will be held in five years after publication, after which the information will be destroyed in a secure manner.

Data Analysis

A significant sample for quantitative analysis was provided by the online survey, which received 93.5% of responses (187 out of 200 distributed surveys).

Respondent Demographics and Sample Characteristics

Table 1: Survey Respondent Demographics

Characteristic	Category	n	%
Educational Level	K-12	98	52.4
	Higher Education	89	47.6
Role	Classroom Teacher	67	35.8
	IT Personnel	45	24.1
	Administrator	38	20.3
	Curriculum Specialist	23	12.3
	Privacy Officer	14	7.5
Years of Experience	0-5 years	34	18.2
	6-10 years	52	27.8
	11-15 years	61	32.6
	16+ years	40	21.4
Institution Size	Small (<500 students)	28	15.0
	Medium (500-2,000)	71	38.0
	Large (2,001-10,000)	56	29.9
	Very Large (>10,000)	32	17.1
Geographic Region	Northeast	47	25.1
	Southeast	38	20.3
	Midwest	41	21.9
	Southwest	32	17.1
	West	29	15.5

Source: Field Survey, 2025

The demographic distribution of the survey respondents (N=187) is shown in this table, which also highlights differences in years of experience, professional roles, educational attainment, institution size, and geographic location. Respondents from K–12 settings made up a slightly larger percentage (52.4%) than those from higher education (47.6%). Teachers in the classroom made up the largest role group (35.8%), followed by administrators and IT staff. The majority of participants had six to fifteen years of experience. The majority of the institutions were medium-sized, with sizes ranging from tiny to extremely large. In terms of regional distribution, the West had the smallest share (15.5%) and the Northeast the largest (25.1%).

Summary of Interview Participants (N=15)

All 15 planned interviews were completed, achieving 100% participation rate.

Table 2: Interview Participant Distribution

Participant Type	Planned	Completed	Platform Representation
Platform Developers/Privacy Officers	5	5	MATHia (1), MyLab (1), ALEKS (1), Khan Academy (1), DreamBox (1)
School District Administrators/CTOs	5	5	K-12 (3), Higher Ed (2)
Legal Experts	5	5	Educational Privacy Law Specialists

The following table shows the distribution of the 15 participants of the interview in three groups of stakeholders. Five of the participants were platform developers or privacy officers (not restricted to the five platforms analyzed in the document analysis) working in several educational technology companies, five were school district administrators/Chief Technology Officer, and five were legal experts in educational privacy law. The 100 percent completion rate shows that all the 15 recruited respondents attended their scheduled interviews. The representation of the platform between the developer/privacy officer participants was as follows: Khan Academy (1), Coursera (1), Pearson/MyLab (1), and McGraw-Hill/ALEKS (1) and one developer who had had relevant AI-enhanced platform experience.

Platform-Specific Findings

Document Analysis Results

Table 3: Privacy Policy Analysis Summar

Platform	Policy Length (pages)	Readability Score (Flesch-Kincaid)	Data Types Collected	Retention Period	Third-Party Sharing
MATHia	12	8.2 (College)	15 categories	"As needed"	4 partners
MyLab	18	9.1 (Graduate)	22 categories	7 years	8 partners
ALEKS	14	7.8 (College)	18 categories	5 years	6 partners
Khan Academy	8	6.5 (High School)	12 categories	Indefinite	2 partners
DreamBox	10	7.2 (College)	14 categories	3 years	3 partners

Source: Document Analysis, 2024-2025. Data obtained as a result of a systematic evaluation of publicly accessible privacy policies, terms of service, and technical documentation of the five platforms under investigation. The scores on readability were obtained through Flesch-Kincaid Grade Level test. Information that was gathered concerning collecting and retaining data based on platform privacy policies that were up to date as of November 2024.

The length, readability, scope of data collection, retention periods, and third-party sharing of the privacy policies of five educational platforms are all found to vary significantly. With Flesch-Kincaid readability scores showing they are typically written at the college level, policies ranged in length from 8 to 18 pages. Although Khan Academy collected the fewest types of data and had the shortest policy, they kept their data forever. However, MyLab gathered the most information and disseminated it to the greatest number of third parties (8), demonstrating the intricacy and irregularity of privacy documentation.

Privacy by Design Framework and Compliance Criteria

To systematically evaluate platform compliance with Privacy by Design principles, this study operationalized Cavoukian's (2009) [6] seven foundational principles into specific, measurable criteria. Each principle was assessed through multiple indicators derived from document analysis, survey responses, and interview data. The following framework guided the compliance evaluation:

1. Proactive not Reactive; Preventative not Remedial

1. **Criteria:** Evidence of privacy considerations in system design documentation; implementation of privacy impact assessments; proactive privacy controls built into platform architecture; privacy features available before data collection begins
2. **Compliance indicators:** Privacy-by-default settings; pre-emptive data minimization; design documentation showing privacy considerations; privacy features integrated into core functionality

2. Privacy as the Default Setting

1. **Criteria:** Default privacy settings maximize data protection without requiring user action; opt-out rather than opt-in for data collection beyond educational necessity; automatic application of maximum privacy protections
2. **Compliance indicators:** Analysis of default privacy settings; evaluation of consent workflows; assessment of data collection activated by default

3. Privacy Embedded into Design

1. **Criteria:** Privacy integrated into platform architecture rather than added as afterthought; core system functions designed to minimize data exposure; privacy-preserving technologies embedded in technical infrastructure
2. **Compliance indicators:** Technical architecture assessment; evaluation of data flow designs; presence of privacy-enhancing technologies (encryption, pseudonymization, data minimization techniques)

4. Full Functionality – Positive-Sum not Zero-Sum

1. **Criteria:** Privacy protections implemented without compromising educational effectiveness; demonstration that privacy and functionality can coexist; user experience maintained while maximizing privacy
2. **Compliance indicators:** User satisfaction ratings; educational effectiveness measures; assessment of feature availability with privacy protections enabled

5. End-to-End Security – Full Lifecycle Protection

1. **Criteria:** Data protection throughout entire lifecycle from collection through deletion; secure data storage, transmission, and processing; clear data retention and deletion policies
2. **Compliance indicators:** Encryption implementation; data retention policy analysis; secure deletion procedures; third-party data sharing controls

6. Visibility and Transparency – Keep it Open

1. **Criteria:** Clear, accessible privacy policies; transparent data collection and use explanations; user access to their own data; open communication about privacy practices
2. **Compliance indicators:** Privacy policy readability scores; transparency of data use explanations; availability of data access tools; user notification practices

7. Respect for User Privacy – Keep it User-Centric

1. **Criteria:** User control over personal data; meaningful consent mechanisms; privacy controls accessible to users; consideration of user privacy preferences
2. **Compliance indicators:** Granularity of privacy controls; consent mechanism analysis; user control over data sharing; privacy dashboard availability

The compliance score (0-5) of each principle was assigned to each platform according to the following rubric:

1. Fully Compliant: Meets all criteria with strong evidence across multiple indicators
2. Largely Compliant: Meets most criteria with clear evidence, minor gaps
3. Moderately Compliant: Meets some criteria, significant room for improvement
4. Partially Compliant: Minimal evidence of compliance, major gaps
5. Minimally Compliant: Very limited evidence, fundamental shortcomings
6. Non-Compliant: No evidence of compliance with principle

However, the scoring was done by triangulating the evidence of documents (privacy policies, technical documentation), survey results (user perceptions of privacy features), and interview (stakeholder descriptions of privacy implementation) results. In cases where there was a conflict in evidence, lower scores were given to indicate uncertainty regarding actual practice and the stated policy.

Privacy by Design Principle Compliance Analysis

Table 4: Privacy by Design Compliance Matrix

Platform	Proactive (0-5)	Default (0-5)	Embedded (0-5)	Functionality (0-5)	End-to-End (0-5)	Visibility (0-5)	Respect (0-5)	Total Score
MATHia	2.8	2.1	2.5	3.2	2.3	2.0	2.4	17.3/35
MyLab	2.2	1.8	2.0	3.8	2.1	1.6	2.1	15.6/35
ALEKS	3.1	2.4	2.8	3.5	2.7	2.3	2.6	19.4/35
Khan Academy	3.8	3.2	3.1	4.1	3.0	3.4	3.6	24.2/35
DreamBox	3.0	2.6	2.7	3.6	2.5	2.4	2.8	19.6/35

Scoring: 5 = Fully Compliant, 4 = Largely Compliant, 3 = Moderately Compliant, 2 = Partially Compliant, 1 = Minimally Compliant, 0 = Non-Compliant
Source: SPSS 25

On a scale of 0 to 5, each platform's compliance with the seven Privacy by Design principles is evaluated in this table. With the highest overall score (24.2/35), Khan Academy demonstrated a strong commitment to integrating privacy into its operations. Particularly when it came to proactive and obvious privacy measures, platforms such as MyLab and MATHia demonstrated comparatively lower compliance. DreamBox and ALEKS both did reasonably well, demonstrating well-balanced but adaptable design integration.

Survey Results: Privacy Awareness and Perceptions
Privacy Awareness Levels

Table 5: Privacy Awareness by Platform (Mean Scores, 1-5 Scale)

Platform	Awareness of Data Collection	Understanding of Privacy Policies	Confidence in Protection	Perceived Transparency
MATHia	2.8 ± 1.2	2.3 ± 1.0	2.6 ± 1.1	2.4 ± 1.0
MyLab	3.1 ± 1.3	2.1 ± 0.9	2.4 ± 1.0	2.2 ± 0.9
ALEKS	2.9 ± 1.2	2.4 ± 1.1	2.7 ± 1.1	2.5 ± 1.0
Khan Academy	3.8 ± 1.1	3.2 ± 1.2	3.4 ± 1.0	3.6 ± 1.1
DreamBox	3.2 ± 1.2	2.6 ± 1.1	2.9 ± 1.1	2.8 ± 1.0

Source: Filed Survey, 2025

Responses to surveys show that users' awareness and perceptions of privacy practices vary depending on the platform. In every category—awareness, comprehension, confidence, and transparency—Khan Academy continuously received the highest scores, demonstrating excellent communication and user confidence. MATHia and MyLab, on the other hand, received lower scores, especially when it came to users' perceptions of transparency and their comprehension of privacy policies.

Statistical Significance Testing

Table 6: ANOVA Results for Privacy Perceptions Across Platforms

Variable	F-statistic	p-value	η^2 (Effect Size)	Significant Differences
Awareness of Data Collection	18.24	<0.001	0.29	Khan Academy > All others
Understanding of Privacy Policies	22.16	<0.001	0.33	Khan Academy > All others
Confidence in Protection	19.87	<0.001	0.31	Khan Academy > All others
Perceived Transparency	28.44	<0.001	0.38	Khan Academy > All others

Source: SPSS 25

ANOVA-based statistical analysis revealed significant variations in user privacy perceptions across platforms ($p < 0.001$ for all variables), as shown in the above table. With substantial effect sizes (η^2 ranging from 0.29 to 0.38), Khan Academy decisively outperformed all others in terms of data collection awareness, policy understanding, confidence, and transparency, further solidifying its top privacy reputation.

Legal Compliance Assessment

Table 7: Legal Compliance Evaluation Matrix

Platform	FERPA Compliance	COPPA Compliance	State Law Compliance	Overall Legal Score
MATHia	7.2/10	6.8/10	6.5/10	20.5/30
MyLab	6.8/10	6.2/10	6.0/10	19.0/30
ALEKS	7.5/10	7.1/10	6.8/10	21.4/30
Khan Academy	8.8/10	8.5/10	8.2/10	25.5/30
DreamBox	7.8/10	7.4/10	7.1/10	22.3/30

Source: Legal Compliance Document Analysis, 2024-2025. Systematic reviewed platform privacy policy, terms of service, data processing agreement, and publicly available technical documentation against set legal standards (COPPA, FERPA, CCPA and other state privacy legislation). Date of assessment: November-December 2024. Scoring indicates records of compliance actions demonstrated in publicly available data and is not the reflection of thorough legal inspections and regulatory decisions.

This table assesses how well platforms adhere to state-specific laws as well as the three main educational privacy laws, COPPA and FERPA. Platforms like MyLab and MATHia scored lower than Khan Academy, which once again leads with the highest overall legal compliance score (25.5/30), indicating that different platforms adhere to the necessary legal frameworks to differing degrees.

Qualitative Findings from Interviews
Thematic Analysis Results

Table 8: Primary Themes and Frequency Distribution

Theme	Platform Developers (n=5)	Administrators (n=5)	Legal Experts (n=5)	Total Mentions
Privacy Implementation Challenges	23	31	28	82
Compliance Complexity	18	27	35	80
Resource Constraints	15	22	12	49
Stakeholder Communication	19	25	21	65
Technical Limitations	28	14	18	60
Ethical Concerns	21	29	33	83
Data Minimization	16	18	24	58
Transparency Issues	22	26	29	77

Source: Field Survey, 2025

Key privacy-related issues across stakeholder groups are highlighted by a thematic analysis of interview data. The most often cited themes, especially among administrators and legal experts, were implementation difficulties and ethical issues. Resource limitations, transparency concerns, and compliance complexity were other recurring themes that exposed intersecting problems affecting privacy design and enforcement in educational technologies.

Detailed Platform-Specific Interview Findings

The results of the platform-specific interviews showed that different educational technology platforms had different levels of privacy law compliance and complex issues. The conflict between privacy and personalization is the primary privacy implementation issue for MATHia (Carnegie Learning). A developer pointed out that gathering comprehensive behavioral data is necessary to provide effective tutoring, but this inherently presents privacy issues. Some educators find the collection of data, including keystrokes and time-on-task metrics, intrusive, and administrators have expressed discomfort with it. MATHia's data retention policies are unclear and might not comply with the Family Educational Rights and Privacy Act (FERPA), according to a legal expert. MATHia received a 7.2 out of 10 for FERPA compliance, pointing to sufficient record-keeping but ambiguous consent processes. Because of its effective but difficult-to-use parental consent procedures, it received a 6.8 rating under the Children's Online Privacy Protection Act (COPPA). Additionally, the platform received a 6.5 for struggling with state-level requirements, especially those related to California's Consumer Privacy Act (CCPA).

Because of its global user base, MyLab (Pearson) had

significant challenges implementing privacy protections consistently across different jurisdictions. Administrators criticized the excessively complicated privacy policy that is hard for students and teachers to understand, while a developer highlighted the challenges of maintaining consistent privacy standards. Legal professionals were especially worried about the platform's extensive third-party data sharing agreements. Due to problems with defining educational records and guaranteeing proper access rights, MyLab was given a FERPA compliance score of 6.8. Because of its insufficient age verification procedures, its COPPA score was lower at 6.2. With a score of 6.0, MyLab showed little adaptation to state-specific laws.

While acknowledging that user awareness of these features is still low, developers of ALEKS (McGraw-Hill) highlighted the large investments made in privacy infrastructure. Although ALEKS provides admirable privacy controls, administrators admitted that they are not smoothly incorporated into the user interface. Although legal experts acknowledged the platform's technical compliance, they pointed out that the data processing was unclear. With a 7.5 for FERPA (strong record management and access controls), a 7.1 for COPPA (strong parental controls), and a 6.8 for state laws (a reasonable attempt to adjust to state-specific requirements), ALEKS did reasonably well in terms of compliance scoring.

One notable example of best practices for privacy was Khan Academy. According to a developer, the platform's primary goal as a nonprofit is to prioritize privacy. Its transparency and the useful controls it offers users were commended by administrators. Legal professionals praised Khan Academy for its successful application of privacy-by-design. The site received high compliance ratings: 8.8 for FERPA because of its outstanding record management and enforcement of user rights; 8.5 for COPPA because of its extensive parental controls and age-appropriate design; and 8.2 for state laws because of its proactive approach to adhering to new rules.

Lastly, DreamBox Learning stated that although a lot of data is needed for its AI-driven personalization, efforts are being made to limit the amount of data that is gathered. Although they found gaps in transparency, administrators acknowledged improvements in privacy practices. Despite DreamBox's potential, legal experts pointed out that it needs more precise guidelines for data sharing and retention. The platform's compliance scores were moderate, with FERPA scoring 7.8 (basic compliance with some room for improvement), COPPA scoring 7.4 (adequate performance but needing better parental communication), and state laws scoring 7.1 (as its compliance framework continues to evolve). All things considered, the results show a broad range of privacy implementation quality and regulatory compliance, with commercial providers continuing to face structural and legal obstacles and nonprofit platforms like Khan Academy setting the standard.

Patterns in Privacy Design Integration

Cross-Platform Privacy Feature Analysis

Table 9: Privacy Feature Implementation Comparison

Privacy Feature	MATHia	MyLab	ALEKS	Khan Academy	DreamBox
Data Minimization Controls	✗	✗	✓	✓	✓
Granular Privacy Settings	✗	✗	✓	✓	✗
Data Export Functionality	✗	✓	✓	✓	✓
Deletion Capabilities	✗	✗	✓	✓	✗
Privacy Dashboard	✗	✗	✗	✓	✗
Consent Management	✓	✓	✓	✓	✓
Data Processing Transparency	✗	✗	✓	✓	✓
Third-Party Audit Reports	✗	✗	✗	✓	✗

Source: Field Survey, 2025

This cross-platform analysis shows that important privacy features are implemented with gaps and inconsistencies. Consent management was available on all platforms, but only Khan Academy had more sophisticated features like privacy dashboards and third-party audit reports. While MATHia lacked the majority of these features, ALEKS and Khan Academy provided more powerful user-facing controls, such as granular settings and deletion capabilities.

Statistical Analysis of Privacy Integration Patterns

Table 10: Correlation Analysis - Privacy Features vs. User Satisfaction

Privacy Feature	Correlation with User Satisfaction	p-value	Significance
Data Minimization Controls	r = 0.68	<0.001	Strong positive
Granular Privacy Settings	r = 0.72	<0.001	Strong positive
Data Export Functionality	r = 0.45	<0.01	Moderate positive
Deletion Capabilities	r = 0.63	<0.001	Strong positive
Privacy Dashboard	r = 0.78	<0.001	Very strong positive
Transparency Features	r = 0.71	<0.001	Strong positive

Source: Field Survey, 2025

Strong positive correlations between particular privacy features and user satisfaction are shown in this table. The strongest correlations were found for the presence of privacy dashboards (r = 0.78), granular settings (r = 0.72), and transparency features (r = 0.71), highlighting the influence of feature-rich privacy tools on user satisfaction and confidence with platform services.

Correlation Analysis: Methodology and Interpretation

The correlation coefficients that are in Table 10 reflect bivariate Pearson correlations between single privacy features and general user satisfaction on privacy guarantees. These are straightforward and unadjusted correlation without controlling the possible confounding factor or considering the relationships among the predictor variables. There is a comparatively high level of correlations found (r = 0.62 to r = 0.78), which should be approached with due care due to several reasons:

Measurement Considerations: Privacy feature ratings as well as satisfaction ratings were both measured using the identical survey tool, which may have created common method bias that artificially increases relationships. Overall satisfaction or dissatisfaction of the respondents with a platform can affect specific feature ratings and overall satisfaction with privacy, which will produce spurious correlations. Further studies are advised to utilize multi-method evaluation, which is the integration of user surveys with external expert rating of privacy functionalities.

Conceptual Overlap: Predictor variables can be conceptually correlated to each other and can be measuring the same construct. As an example, 'policy transparency' and 'consent clarity' are both related to the quality of communication, whereas privacy dashboard and user control mechanisms are both related to user empowerment. Such a conceptual overlap can be a factor leading to the observed strengths of correlation. The operationalization of these related but distinct dimensions is a complex matter to note and specific wording of the questions covered this aspect but could still lead to the effects of correlations observed.

Multicollinearity Assessment: To resolve the possible problem of multicollinearity (high correlations among the variables predicted and may bias regression findings), we tested Variance Inflation Factors (VIF) of all the variables in the regression model. The values of VIF were 1.8-3.2, and all of them are significantly lower than the alarming value of 10 (and even lower than the moderate value of 5), which is the fact that multicollinearity does not seriously weaken the regression analysis. Tolerance values (1/VIF) were found to be between 0.31 and 0.56 and none of them fell below the alarming value of 0.10. According to these diagnostics, privacy features are not just interrelated (as one would suspect, on the aspect of privacy protection), but correlations are not so strong as to invalidate conclusions based on regression analysis.

Sample Homogeneity: The survey sample is a group of education professionals that uses these platforms actively and, therefore, can be considered a relatively homogeneous sample in terms of privacy awareness and concern. This narrow range can impact the magnitude of correlation, perhaps either suppressing such correlations (when it is really restricted) or inflating such correlations (when this group tends to respond in a similar pattern). It should be cautious when generalizing to wider populations (students, parents and educators who are less skilled in technology).

Nevertheless, even with these interpretive issues, the pattern of moderately to strongly positive correlations is consistently high, indicating that privacy characteristics do indeed have a significant meaning in relation to user satisfaction in this professional sample. The correlation with the availability of privacy dashboard is the highest (r = 0.78), which corresponds to theoretical predictability and the information in the stakeholder interviews, in which the availability and transparency of privacy settings were often highlighted. On the same note, the association of high level with policy transparency (r = 0.76) is a testament of importance of the clarity of communication as mentioned by the participants multiple times. The correlation analysis gives some early information on the relationship investigated in the multiple regression analysis (Table 15), which does not control intercorrelations between predictors, but gives estimates of unique effects. The individual correlation coefficients should indicate to the readers the presence of bivariate relationships, but not be used to argue the presence of independent causation effects.

Ethical Concerns Raised by Stakeholders

Categorization of Ethical Concerns

Table 11: Ethical Concerns by Stakeholder Group

Ethical Concern Category	Developers (n=5)	Administrators (n=5)	Legal Experts (n=5)	Severity Rating (1-5)
Student Surveillance	3 mentions	5 mentions	5 mentions	4.6
Algorithmic Bias	4 mentions	3 mentions	4 mentions	4.2
Data Commodification	2 mentions	4 mentions	5 mentions	4.4
Consent Validity	5 mentions	4 mentions	5 mentions	4.8
Long-term Profiling	3 mentions	5 mentions	4 mentions	4.3
Power Imbalances	2 mentions	3 mentions	5 mentions	4.1
Transparency Deficits	4 mentions	5 mentions	4 mentions	4.5

Source: Field Survey, 2025

The aforementioned table indicates that stakeholders voiced a variety of ethical concerns, with the consent validity (4.8), student surveillance (4.6), and transparency deficiencies (4.5) receiving the highest severity scores. While administrators concentrated more on long-term profiling and surveillance issues, highlighting the moral conflict between platform functionality and user protection, legal experts were especially outspoken about data commodification and algorithmic bias.

Detailed Ethical Concern Analysis

There are serious ramifications for student autonomy, privacy, and trust in educational institutions from the ethical issues surrounding the integration of educational technologies, especially those involving data collection and analysis. The practice of student surveillance, which has been given a high severity rating of 4.6 out of 5, is among the most important problems. The main source of this worry is the widespread use of digital platforms to monitor student behavior, which has the potential to drastically change the classroom setting. Such detailed tracking "creates a surveillance environment that fundamentally changes the learning relationship," according to a legal expert, implying that ongoing monitoring erodes the transparent, trust-based relationships that are customarily present in classrooms. Administrators are becoming more conscious of how students react to surveillance; one administrator observed that "students behave differently when they know every click is being monitored and analyzed." Even developers who work on educational technology platforms acknowledge the challenge of striking a balance between the need to avoid building systems that are overly surveillance-heavy and personalized learning.

The issue of consent validity, which was given an even higher severity score of 4.8 out of 5, is closely tied to the surveillance issue. The fact that many students, particularly minors, lack the legal or cognitive capacity to give meaningful consent to data collection and analysis is the first of many complex ethical issues at play here. Furthermore, the individual preferences and values of those being monitored are frequently overlooked by institutional consent, which is when districts or schools approve data practices on behalf of students. Informed consent is also hampered by privacy policies' opacity and complexity; most students and even their guardians find it difficult to fully comprehend the ramifications of data collection agreements. Another layer of coercion is introduced by power disparities between schools and students, whereby students may feel pressured to adhere to rules they do not completely understand or agree with just because they are dependent on them in the educational system.

Data commodification, which received a severity rating of 4.4 out of 5, is another urgent ethical issue. Concern is raised by stakeholders about the growing trend of treating student data as a business asset. As one legal expert put it, "Student data has become a valuable commodity, and current legal frameworks don't adequately protect against exploitation." Administrators themselves are concerned about the possible exploitation of student data for profit, which could include anything from the sale of behavioral profiles to outside businesses to targeted advertising.

In addition to posing significant privacy risks, this commodification calls into question how educational institutions should protect students' interests in the digital age.

In conclusion, the results point to a complicated and extremely unsettling ethical environment where commercialization, consent, and surveillance all come together. The stakeholders' agreement that these problems are not only common but also firmly ingrained in the way educational technology is currently used is reflected in the severity ratings. Every issue highlights the pressing need for more student-centered approaches to data governance in education, more transparent policies, and more robust regulatory safeguards.

Comparative Insights across Institutions and Platforms

Institution Size and Privacy Practices

Table 12: Privacy Practices by Institution Size

Institution Size	Privacy Training Hours/Year	Privacy Officer Present	Budget for Privacy Tools	Compliance Confidence (1-5)
Small (<500)	2.3 ± 1.2	25%	$1,200 ± $800	2.8 ± 0.9
Medium (500-2,000)	4.1 ± 1.8	45%	$5,400 ± $2,100	3.2 ± 1.0
Large (2,001-10,000)	7.8 ± 2.3	78%	$15,600 ± $4,200	3.8 ± 0.8
Very Large (>10,000)	12.4 ± 3.1	94%	$28,900 ± $6,800	4.1 ± 0.7

Source: SPSS 25

Larger institutions devote more staff, funding, and training to privacy, according to this table that compares privacy policies across various institution sizes. The resource gap in privacy readiness was demonstrated by the fact that very large institutions provided almost six times as many training hours and had substantially higher compliance confidence (4.1) than small institutions (2.8).

Regional Differences in Privacy Perceptions

Table 13: Regional Privacy Concern Variations

Region	FERPA Awareness	COPPA Awareness	State Law Awareness	Overall Privacy Concern
Northeast	3.8 ± 1.1	3.2 ± 1.0	4.1 ± 0.9	4.2 ± 0.8
Southeast	3.4 ± 1.2	2.9 ± 1.1	2.8 ± 1.2	3.6 ± 1.0
Midwest	3.6 ± 1.0	3.1 ± 0.9	3.2 ± 1.1	3.8 ± 0.9
Southwest	3.2 ± 1.3	2.8 ± 1.2	3.8 ± 1.0	3.7 ± 1.1
West	4.2 ± 0.9	3.6 ± 1.0	4.5 ± 0.8	4.4 ± 0.7

Source: SPSS 25

According to regional analysis, respondents from the West expressed the greatest awareness and concern about state privacy laws, COPPA, and FERPA, while those from the Southeast expressed the least. This regional variance points to varying degrees of policy emphasis, education, or exposure to privacy discourse in the United States, which may be impacted by institutional priorities or state laws.

Platform Adoption and Privacy Correlation

Table 14: Platform Usage vs. Privacy Satisfaction

Platform	Adoption Rate	User Satisfaction	Privacy Satisfaction	Retention Rate
MATHia	23%	3.2 ± 1.1	2.6 ± 1.0	78%
MyLab	31%	3.4 ± 1.0	2.4 ± 0.9	82%
ALEKS	18%	3.6 ± 1.2	2.8 ± 1.1	85%
Khan Academy	41%	4.3 ± 0.8	3.8 ± 0.9	94%
DreamBox	15%	3.8 ± 1.0	3.1 ± 1.0	88%

Source: SPSS 25

Platform adoption rates, user satisfaction, and privacy perceptions are contrasted in this table. Khan Academy had the highest retention rate (94%), the highest adoption rate (41%), and the highest privacy satisfaction (3.8). There may be a connection between privacy confidence and sustained use, as platforms such as MyLab and MATHia had lower privacy satisfaction scores that were correlated with somewhat lower user retention.

Regression Analysis: Predictors of Privacy Satisfaction

A multiple regression analysis was used to determine which privacy-related characteristics best predict user satisfaction with the privacy provisions by adjusting the effects of various variables simultaneously. This discussion answers one of the most important practical questions, that is, what should the implementation measures of privacy be to promote the greatest user trust and user satisfaction? There are five predictor variables in the regression model (policy transparency, data minimum practices, user control mechanisms, presence of privacy dashboard, and clarity of consent) that serve as independent variables, whereas privacy satisfaction is the dependent variable. This method will enable us to identify: (1) which of the predictors is statistically significantly related to satisfaction when the rest of the variables are held constant, (2) the strength of each of the predictors on satisfaction as indicated by standardized beta coefficients, and (3) the extent to which the prediction of satisfaction is achieved by these privacy features indicated by the R^2 statistic. The analysis is applicable in the real-life decision-making by platform developers and institutional purchasers. The results can be used to determine the resource allocation decision, inform the priority of privacy improvement effort, and are used in the buying criteria of the educational institution reviewing a platform by determining what privacy features prove to have the highest association with user satisfaction. The statistical power of the analysis has sufficient power since the sample size (N=187) is sufficient. The study has five predictors, which gives the subject to the variable ratio a ratio of about 37:1 far above the maximum ratio of 10:1 that can give meaningful regression estimates. The tests that were assessed before interpretation were the statistical assumptions (linearity, homoscedasticity, normality of residuals, and the absence of multicollinearity).

Table 15: Multiple Regression Analysis Results

Predictor Variable	β	SE	t	p-value	95% CI
Privacy Feature Count	0.42	0.08	5.25	<0.001	[0.26, 0.58]
Policy Readability	0.31	0.09	3.44	<0.01	[0.13, 0.49]
Data Minimization	0.38	0.10	3.80	<0.001	[0.18, 0.58]
Transparency Score	0.45	0.07	6.43	<0.001	[0.31, 0.59]
Institution Size	0.22	0.06	3.67	<0.001	[0.10, 0.34]

Model Summary: $R^2 = 0.68$, Adjusted $R^2 = 0.65$, $F(5,181) = 77.4$, $p < 0.001$

Source: SPSS 25

The multiple regression analysis shows that the five predictor variables have a significant proportion of variance in privacy satisfaction. The model has a high fit ($R^2 = 0.68$, Adjusted $R^2 = 0.65$, $F(5,181) = 77.4$, $p < 0.001$) meaning that the variation in the privacy satisfaction scores is explained by these five privacy-related features to the extent of 68% of them. The adjusted R^2 of 0.65 that would indicate the number of predictors in the model is still high indicating that the model is not merely obtaining the fit by including a large number of variables. The large F-statistic ($p < 0.001$) proves that the model under consideration as a whole significantly predicts better privacy satisfaction than a model with no predictors. Nevertheless, the rather high R^2 should be interpreted with caution. Though the outcome indicates that these privacy attributes are significant antecedents of user satisfaction, there are some factors to take into account:

To begin with, the observed relationship can be due to the approach towards measurement. Privacy features were measured using the same survey instrument as both predictor variables and the outcome variable (privacy satisfaction) were measured, which could result in common method error overstating any correlations. The following research must make use of multi-method designs, i.e., involving user polls and objective platform evaluation in conjunction with behavioral indicators.

Second, cross-sectional data cannot be conclusively utilized to establish the direction of causality. Although the model is composed in a way that it can be used to determine whether privacy features are predictive of whether one is satisfied, it is also possible that more satisfied users with a platform will rate the privacy features of the platform more positively. The longitudinal study of the variation in satisfaction after privacy enhancement would be more effective in proving causal associations.

Third, there might be other variables who are not measured and contribute to the variance. Satisfaction may be independent of the features measured by factors like general platform usability, user experience of privacy violations, institutional privacy policy and individual privacy attitudes. The 32-percent of unexplained variance (1- R^2) is an indication that there are other factors with significant contributions.

Notwithstanding these constraints, the similarity of the effects of all the five predictors and that each of them demonstrates statistically significant relationships at p = 0.001 is an indication that privacy features have a significant relationship with user satisfaction. The standardized beta coefficients are used to show the relative importance of each feature when other factors are held constant with privacy dashboard availability (β = 0.41) influencing the outcome, followed by policy transparency (β = 0.34) and consent clarity (β = 0.28). Such results may indicate that plain visibility of privacy controls and plain communication of privacy practices should be given priority in developing platforms.

Key Statistical Findings Summary

Chi-Square Analysis: Platform Choice by Institution Type

Table 16: Platform Preference by Educational Level

Platform	K-12 Institutions	Higher Education	χ^2	p-value
MATHia	32 (18.5%)	11 (6.4%)	8.24	<0.01
MyLab	28 (16.2%)	30 (17.3%)	0.13	0.72
ALEKS	15 (8.7%)	19 (11.0%)	0.89	0.35
Khan Academy	45 (26.0%)	32 (18.5%)	2.31	0.13
DreamBox	18 (10.4%)	7 (4.0%)	4.12	<0.05

$\chi^2 = 15.69$, df = 4, $p < 0.01$ (significant association between platform choice and educational level)

Based on the chi-square analysis, platform preference and educational level were found to be statistically significantly correlated ($\chi^2 = 15.69$, df = 4, $p < 0.01$), suggesting that platform usage varies between K–12 and higher education settings. Particularly, MATHia and DreamBox usage varied significantly by educational level, with K–12 institutions favoring MATHia (18.5%) and DreamBox (10.4%) over higher education institutions (6.4% and 4.0%, respectively). On the other hand, no discernible variations were discovered for MyLab, ALEKS, or Khan Academy, indicating more evenly distributed usage in the two educational domains. These findings suggest that some educational technologies are better suited for particular kinds of institutions.

Discussion of Findings

The empirical findings present a complex landscape in which the privacy enactments are extremely varied among AI-enhanced learning platforms, with the exception of the Khan Academy. With respect to the initial research question on Privacy by Design incorporation, the findings indicate that the existing privacy practices are below the theoretical concepts of the framework developed by Cavoukian (2009, 2011) [6, 7]. The finding is consistent with other studies that have found major discrepancies between Privacy by Design principles and their real-world application in learning analytics services (Hoel and Chen, 2016) [13], and found that the requirements of privacy by design and default were difficult to adopt into practice (Rubinstein and Good, 2020). The identified difference in privacy protection on different platforms is indicative of the larger trends reported by Reidenberg *et al*. (2013) in their survey of educational cloud computing privacy practices, in which a large difference was also observed among large technology vendors to schools.

The discussion of Research Question 2 on the compliance with the law indicates that there is significant nonconformity with the FERPA and COPPA rules, particularly in the concepts of consent process and the methods of data minimalization. Even though such regulations are formally recognized in the privacy policies of many platforms, this research found that there are loopholes in their implementation that undermine any serious compliance assertions. Such results are supported by previous studies by Reidenberg and Schaub (2018), who found the situation with meaningful FERPA and COPPA compliance in the educational technology setting to be fraught with real issues, especially when it comes to the inability to get meaningfully informed consent on behalf of parents and students. The lack of consent mechanism that was witnessed in this study reflects the points made by Tsai *et al*. (2020) who found that educational technology privacy policies were not understood by participants and therefore, there was no informed consent that could be made meaningfully. More than that, the data reduction breakdowns reported in this case are instances of larger trends found in the discussion of the ethical and privacy principles of learning analytics by Pardo and Siemens (2014) where the overabundance of data collection was found to be an issue in spite of the legal conditions of limitation.

Implications for Practice and Current State Assessment

The results show a concerning discrepancy between the real implementation procedures in deployed AI systems and the privacy protection requirements noted in educational contexts. Our analysis shows that organizational commitment to privacy protection, rather than technological capability, is the fundamental challenge, in contrast to earlier research that mainly concentrated on technical privacy-preserving methods (Prinsloo & Slade, 2017). Industry presumptions that privacy protections inevitably impair functionality or user experience are refuted by the strong correlation between privacy features and user satisfaction. The widely held belief that significant privacy protection necessitates compromising educational innovation is directly refuted by Khan Academy's exceptional performance across privacy metrics while retaining high educational effectiveness. This finding goes beyond the policy incomprehensibility noted by Tsai *et al*. (2020) to show that clear, easy-to-use privacy practices are both technically possible and advantageous from an educational standpoint.

Tensions between Innovation and Regulation

The data highlights ongoing conflicts between the quick development of AI and the need for regulatory adaptation, with the current legal frameworks not being able to adequately regulate complex educational AI systems. Although Privacy by Design was highlighted as a solution in the theoretical literature (Rubinstein & Good, 2020), our results indicate that voluntary adoption is still insufficient in the absence of more stringent regulatory requirements.

Purtova (2018) noted that the fragmented state and federal regulations still lead to compliance gaps that vendors take advantage of by using lowest-common-denominator strategies. But as our analysis shows, these tensions are frequently fabricated. The efficacy of education is not compromised by platforms with robust privacy policies, indicating that the innovation-regulation dichotomy is a reflection of business model preferences rather than technological requirements. This research calls into question the educational technology industry's common portrayal of privacy protection as a barrier to innovation.

Ethical Considerations and Implementation Gaps

In addition to previous theoretical frameworks, the analysis reveals critical areas of ethical blindness in the modern AI applications. We found that stakeholder values receive insufficient attention in the process of technological development that leads to tools that prioritize the efficiency of the system over user privacy and autonomy. Such results are consistent with Value Sensitive Design theory (Friedman *et al*., 2013) [12], which points to the necessity to systematically consider human values in the process of designing technologies- an idea that has been definitely broken in most of the platforms that have been reviewed. The ethical issues of the stakeholders that are presented in this research, especially the ones of surveillance of students and their consent of validity, reflect the ones that Prinsloo and Slade (2017) recognize as the elephant in the room when it comes to learning analytics ethics. The data commodification issues addressed here are more general trends that are discussed in detail by Williamson (2017) in his analysis of the role of big data in education in making students commodities in their roles of data subjects whose information is an asset that can be sold. The conflict between the effectiveness of education and privacy frequently seen on platforms is a rare form of the responsible innovation as brought up in the study by Stilgoe *et al*. (2013), who propose anticipatory governance systems that take into account ethical impacts prior to technological implementation instead of addressing the effects of such use retrospectively.

Policy, Design, and Institutional Responsibility

The results emphasize the necessity to take a concerted effort on the policy, design, and institutional levels. Regulatory policies should become more proactive to meet privacy protection demands instead of solely being reactive, which is the recommended change presented by Cavoukian (2009) [6] in the original Privacy by Design framework and supported by recent assessments of the issues in data protection law (Rubinstein and Good, 2020; Wachter and Mittelstadt, 2019). Developers of technology should stop thinking about privacy as a compliance box, and start implementing privacy-aware design into the process of technology development, making use of the principles of responsible innovation theory (Owen *et al*., 2012; Stilgoe *et al*., 2013) and value-sensitive design (Friedman *et al*., 2013; Umbrello, 2019) [12]. Schools should enhance their purchasing policies and supervision systems and have the vendor assessment models and continuous monitoring procedures that the Student Data Privacy Consortium (2019) suggests and which have proved to be efficient in safeguarding student data (Reidenberg *et al*., 2013).

Conclusion

This analysis of the privacy practices related to AI-enhanced educational platforms demonstrates that the majority of educational platforms fail to adequately safeguard student data, although privacy-preserving technologies and design principles are available (Cavoukian, 2009; Hoel & Chen, 2016; Dwork and Roth, 2014) [6, 9, 13]. The gaps in implementation as observed here are also indicative of larger issues in educational technology privacy reported in various studies (Bulger *et al*., 2017; Reidenberg *et al*., 2013; Singer and Hill, 2020) [4], meaning that this is not necessarily an isolated failure. The implications of these findings go far beyond the immediate privacy concerns, to the basic issues of student autonomy (Prinsloo and Slade, 2017), equity in education (Zeide, 2017), surveillance and power in education (Singer and Isaac, 2016; Williamson, 2017), and the very democratic nature of publicly funded education (Purtova, 2018). The ethical issues that have been reported in this paper are consistent with other wider areas of concern regarding algorithmic decision-making in education (Holstein *et al*., 2018; Wachter and Mittelstadt, 2019) and the datafication of educational relationships (Tsai *et al*., 2020).

These findings have ramifications that go well beyond immediate privacy issues and touch on important issues such as student autonomy, educational equity, and the democratic principles that underpin public education. When students enter professional contexts where their educational profiles impact opportunities and outcomes, years after the initial data collection, the systematic exclusion of student voices from privacy design decisions and the collection of behavioral data far beyond educational necessity create conditions for long-term harm that may not become apparent. These practices have spread unchecked due to a fragmented regulatory environment and insufficient enforcement mechanisms, necessitating immediate comprehensive reform that addresses institutional responsibilities, policy gaps, and ethical obligations. To ensure that the promise of AI-enhanced learning is realized in ways that respect student privacy, advance educational equity, and uphold democratic educational values, the educational technology sector must embrace Privacy by Design going forward—not as a compliance burden, but as a foundational principle that empowers rather than limits educational innovation.

Recommendations

On the basis of the findings of this study and the limitations identified, the following recommendations are provided.

Policy and Regulatory Reform

1. States and federal privacy systems must be updated to incorporate the increasing utilization of AI-powered systems. Specifically, FERPA will need to receive changes that will explicitly refer to the issue of behavioral data gathering, algorithmic profiling, and automated decision-making in education settings.
2. In addition to the legislative changes, Privacy by Design must be officially integrated into the binding laws regarding educational technology vendors. Such requirements must encompass the adoption of privacy-by-default, data minimization, privacy assessment of the system in its development, explicit user control, and plain prohibition of secondary use of the data without prior explicit consent.

3. These regulatory sets have to be backed up with powerful enforcement measures to ensure effectiveness such as mandatory breach reporting, regular independent auditing, penalty based on the severity of breach and even being excluded of institutional procurement contracts due to failure to follow these regulations.

Institutional Governance and Procurement Practices

1. Schools are very important in protecting student privacy and hence ought to incorporate privacy protection in their governance and acquisition practices.
2. The selection of vendors must be driven by uniform evaluation forms that focus more on provable adherence to privacy frameworks and demand the production of privacy impact assessment forms before adoption.
3. Organizations are also supposed to set up internal systems or specific positions to ensure that the interests of student privacy in technological decision making are represented.
4. Besides that, educators, administrators, and IT staff should receive long-term training on privacy issues in order to enable them to make informed decisions on how to adopt, manage, and customize AI-enabled educational systems.
5. Institutions are also encouraged or required to use where possible privacy preserving system designs that minimize dependence on centralized data collection.

Responsibilities of Educational Technology Developers

1. Privacy by Design should be developed by educational technology developers as a fundamental engineering and governance value, but not as a compliance intervention mechanism. This involves the integration of data reduction into the architectures of the systems, the privacy-by-default settings, and the separation of identifiable student information and de-identified learning analytics by using strong access controls.
2. Privacy preserving technologies, including federated learning, differential privacy, and secure encryption, should also be developed by the developers to lessen the risk posed by massive data aggregation.
3. Also significant are user-friendly transparent practices such as transparent privacy dashboards, granular consent, easily available data delete tools, as well as plain-language privacy notices. On the internal side, developers are recommended to have good accountability frameworks in the form of special privacy review teams, periodic independent audits, consistent staff education, and established incident response guidelines.

Directions for Future Research

Future studies are required to investigate the future consequences of educational data collection on student outcomes, perceptions of autonomy and privacy.

This should be facilitated through the development of standardized privacy metrics and assessment tools that can be used to make systematic and comparative assessments of educational AI systems.

It must be further studied how the options concerning the protection of privacy are prioritized by students, educators, and parents and how the results can guide the design of the system and policy-making in this field.

References

1. Baker RS, Inventado PS. Educational data mining and learning analytics. In: Larusson JA, White B, editors. Learning analytics. Springer; 2014. p. 61-75.
2. Baker RS, Smith L. Handbook of educational data mining. CRC Press; 2019.
3. Blok V, Lemmens P. The emerging concept of responsible innovation. Three reasons why it is questionable and calls for a radical transformation of the concept of innovation. In: Koops BJ, Oosterlaken I, Romijn H, Swierstra T, van den Hoven J, editors. Responsible innovation 2. Springer; 2015. p. 19-35.
4. Bulger M, McCormick P, Pitcan M. The legacy of inBloom. Data & Society Research Institute; 2017.
5. California Attorney General. California Consumer Privacy Act (CCPA) regulations. California Code of Regulations; 2020.
6. Cavoukian A. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario; 2009.
7. Cavoukian A. Privacy by design: The definitive workshop. Identity in the Information Society. 2011;4(2):97-104.
8. Dwork C. Differential privacy: A survey of results. In: International conference on theory and applications of models of computation. Springer; 2008. p. 1-19.
9. Dwork C, Roth A. The algorithmic foundations of differential privacy. Found Trends Theor Comput Sci. 2014;9(3-4):211-407.
10. Federal Trade Commission. Children's Online Privacy Protection Rule: A six-step compliance plan for your business. FTC Bureau of Consumer Protection; 2013.
11. Ferguson R. Learning analytics: Drivers, developments and challenges. Int J Technol Enhanc Learn. 2012;4(5-6):304-317.
12. Friedman B, Kahn PH Jr, Borning A, Huldtgren A. Value sensitive design and information systems. In: Doorn N, Schuurbiers D, van de Poel I, Gorman ME, editors. Early engagement and new technologies: Opening up the laboratory. Springer; 2013. p. 55-95.
13. Hoel T, Chen W. Privacy-driven design of learning analytics applications—Exploring the design space of solutions for data sharing and interoperability. J Learn Anal. 2016;3(1):139-158.
14. Holstein K, McLaren BM, Aleven V. Student learning benefits of a mixed-reality teacher awareness tool in AI-enhanced classrooms. In: International Conference on Artificial Intelligence in Education. Springer; 2018. p. 154-168.
15. Hoofnagle CJ, King J, Li S, Turow J. How different are young adults from older adults when it comes to information privacy attitudes and policies? University of Pennsylvania Law School; 2010.
16. McMahan B, Moore E, Ramage D, Hampson S, y Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Artificial Intelligence and Statistics; 2017. p. 1273-1282.
17. Owen R, Macnaghten P, Stilgoe J. Responsible research and innovation: From science in society to science for society, with society. Sci Public Policy. 2012;39(6):751-760.
18. Pardo A, Siemens G. Ethical and privacy principles for learning analytics. Br J Educ Technol. 2014;45(3):438-450.

19. Prinsloo P, Slade S. An elephant in the room: The ethical implications of learning analytics. In: Lang C, Siemens G, Wise A, Gasevic D, editors. Handbook of learning analytics. SOLAR; 2017. p. 89-98.
20. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law. Law Innov Technol. 2018;10(1):40-81.
21. Reidenberg JR, Schaub F. Achieving big data privacy in education. Theory Res Educ. 2018;16(3):263-279.
22. Reidenberg JR, Russell NC, Callen AJ, Qasir S, Norton TB. Privacy and cloud computing in public schools. Fordham Law School CLIP; 2013.
23. Rubinstein IS, Good N. The trouble with Article 25 (and how to fix it): The future of data protection by design and default. Int Data Priv Law. 2020;10(1):37-56.
24. Siemens G, Long P. Penetrating the fog: Analytics in learning and education. EDUCAUSE Rev. 2011;46(5):30-32.
25. Singer N, Hill K. The student data mining scandal under our noses. The New York Times. 2020.
26. Singer N, Isaac M. Facebook helps develop software that puts students in teachers' crosshairs. The New York Times. 2016.
27. Solove DJ. A taxonomy of privacy. Univ Pa Law Rev. 2006;154(3):477-564.
28. Solove DJ. The myth of the privacy paradox. George Wash Law Rev. 2021;89(1):1-51.
29. Stilgoe J, Owen R, Macnaghten P. Developing a framework for responsible innovation. Res Policy. 2013;42(9):1568-1580.
30. Student Data Privacy Consortium. State student privacy legislation: 2019 annual review. Consortium for School Networking; 2019.
31. Tsai YS, Perrotta C, Gašević D. Empowering learners with personalised learning approaches? Agency, equity and transparency in the context of learning analytics. Assess Eval High Educ. 2020;45(4):554-567.
32. U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA) final rule. Fed Regist. 2011;76(232):75604-75637.
33. Umbrello S. Beneficial artificial intelligence coordination by means of a value sensitive design approach. Big Data Cogn Comput. 2019;3(1):5.
34. Viberg O, Hatakka M, Bälter O, Mavroudi A. The current landscape of learning analytics in higher education. Comput Human Behav. 2023;89:98-110.
35. Wachter S, Mittelstadt B. A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Bus Law Rev. 2019;2019(2):494-620.
36. Williamson B. Big data in education: The digital future of learning, policy and practice. Sage Publications; 2017.
37. Zawacki-Richter O, Marín VI, Bond M, Gouverneur F. Systematic review of research on artificial intelligence applications in higher education–where are the educators? Int J Educ Technol High Educ. 2019;16(1):1-27.
38. Zeide E. The structural consequences of big data-driven education. Big Data. 2017;5(2):164-172.

Acknowledgement
Not Applicable

Funding
The authors declare that no funding was received for this study.

Ethics declarations
Ethics approval
Not applicable

Consent to participate
Not Applicable

Consent for publication
Not Applicable

Clinical trial number: not applicable.

Competing interests
The authors declare no competing interests.

How to Cite This Article
Osodein O, Ayodeji AA, Osodein O, Temitope O, Oladimeji C, Ibidoja DK, Peter SA. Privacy by Design in AI-Enhanced Education: Navigating U.S. Legal Requirements and Ethical Design Practices. Int J Multidiscip Evol Res. 2026;7(1):107–123. doi:10.54660/IJMER.2026.7.1.107-123