Exploring the Intersection of Student Consent, Privacy, and Data Analytics in Adaptive Learning Platforms

Group Members: Jesse Cox, Mayumy Cordova, Beth McBride

Abstract

Adaptive learning platforms have changed how students use educational technology by using data analytics to personalize everything from instruction to the set of questions used to assess knowledge. However, these platforms also raise ethical and legal concerns related to student consent, data privacy, and algorithmic transparency. This project will examine how student data is collected, stored, and used, analyzing whether current consent mechanisms are adequate. We will also study how privacy protections are enforced and the broader implications of algorithm-driven decision-making in education, especially related to K-12 education. To do this we will apply theories and frameworks from Nissenbaum (2011), Solove (2002), and Mulligan et al. (2016) to assess whether adaptive learning platforms for K-12 audiences align with best practices for privacy and security. We will also draw on regulatory and policy frameworks like FERPA, GDPR, and COPPA, as well as different ethical principles like informed consent and algorithmic fairness.

Introduction

Adaptive learning platforms have significantly transformed the landscape of K-12 education, leveraging sophisticated algorithms and data analytics to tailor educational content to individual students' needs. These platforms continually assess a student's progress and dynamically adjust material, attempting to improve a student's learning experience by adjusting to their learning pace and preferences (Baker & Yacef, 2009; Long & Siemens, 2014). This personalized approach has the potential to improve educational outcomes (Pane, et al., 2015; Baker & Yacef, 2009).

The importance of understanding how student consent, privacy, and adaptive learning platforms relate to each other is increasingly important due to the rapid adoption of online learning technologies during and after the COVID-19 pandemic. Decreases in state K-12 test scores in reading and math since 2020 have heightened the need for effective educational interventions, positioning adaptive learning technologies as a critical tool to address these challenges (National Center for Education Statistics, 2022).

The need to mitigate learning loss has driven many schools to adopt adaptive learning technologies in the years since 2020. However, the rapid development of the adaptive systems has often outpaced the development of comprehensive privacy frameworks and ethical guidelines, leading to potential risks for students' privacy and autonomy.

Main Question and Objectives

This paper explores the main question: How is power and responsibility distributed between learners, educators, institutions, and platform providers in the context of adaptive learning platforms in K-12 education?

To address this question, we will examine how student data is collected, stored, and used, analyzing whether current consent mechanisms are adequate. We will also study how privacy protections are enforced and the broader implications of algorithm-driven decision-making in education.

Background on Adaptive Learning Platforms

Adaptive learning platforms are designed to personalize the educational experience through real-time data collection, content adjustment, and performance tracking (Brusilovsky & Millan, 2007). These types of platforms use various models, such as Bayesian knowledge tracing, item response theory, and collaborative filtering, to continuously assess and adapt to a student's learning needs (Baker & Yacef, 2009). In more recent years, these platforms have begun to use machine learning models and large language models.

Some specific adaptive learning platforms show examples of how these technologies work:

- **DreamBox Learning:**
    - ***How it works:*** DreamBox is an adaptive learning platform focused on K-8 mathematics. It uses real-time data to adjust the difficulty of math problems and the sequence of lessons based on each student's performance. DreamBox analyzes students' responses, the time taken to solve problems, and their interaction patterns to provide personalized feedback and adjust the learning path.
    - ***Key features:*** Interactive and engaging lessons, immediate feedback, and a personalized learning path that adapts to each student's strengths and weaknesses.
    - ***Users:*** As of 2023, DreamBox Learning serves over 6 million students and 600,000 educators across the United States, Canada, and Mexico (Soper, 2023).

- **i-Ready:**
    - ***How it works:*** i-Ready combines diagnostic assessments with personalized instruction in reading and mathematics for K-12 students. The platform uses adaptive assessments to identify students' skill levels and instructional needs. Based on the assessment results, i-Ready delivers materials that target specific areas for improvement.
    - ***Key features:*** Adaptive diagnostic assessments, individualized lesson plans, and progress monitoring.
    - ***Users:*** As of 2025, i-Ready is used by more than 13 million students in schools across the United States (Curriculum Associates, 2025).

- **Knewton:**
    - ***How it works:*** Knewton provides adaptive learning technology that integrates with various educational content providers to offer personalized learning experiences. The platform uses machine learning algorithms to analyze students' interactions with the content and predict their future performance. Knewton adjusts the content delivery based on these predictions to optimize learning outcomes.
    - ***Key features:*** Content agnostic platform, predictive analytics, and real-time adaptation of learning materials.
    - ***Users:*** As of 2025, Knewton's technology has reached over 40 million students (Knewton, 2025).

These examples demonstrate a few of the approaches used by adaptive learning platforms to personalize education. By using data and advanced algorithms, these platforms are aiming to create a more engaging and effective learning experience tailored to student needs.

Legal and Regulatory Frameworks

To understand the ethical and legal implications of adaptive learning platforms, we must consider the relevant regulatory frameworks that govern student data privacy. We will use these frameworks as a basis for our analysis later in this paper. Key regulations include:

- **Family Educational Rights and Privacy Act (FERPA)**: This U.S. federal law protects the privacy of student education records and grants parents certain rights regarding their children's education records.
- **Children's Online Privacy Protection Act (COPPA)**: This U.S. federal law imposes certain requirements on operators of websites or online services directed to children under 13 years of age, including obtaining verifiable parental consent before collecting personal information from children.
- **General Data Protection Regulation (GDPR)**: This European Union regulation sets stringent data protection and privacy requirements for individuals within the EU, including provisions relevant to the processing of children's data.

Analysis Using Solove, Nissenbaum, Mulligan et. al. etc.

Solove

Solove's taxonomy has a robust framework to outline privacy risks into information collection, processing, dissemination and invasion. Throughout these framework analysis, gaps in privacy protections and accountability will be identified to reveal where current systems are failing students and where policy needs to be improved. Adaptive learning platforms collect vast amounts of data such as time spent to resolve questions and response accuracy. These platforms often gather information passively, without clearly informing students or parents about the full scope of collection. For example, DreamBox analyses time-on-task and click patterns to adjust the difficulty of lessons in real time, but it is not always transparent about what behavioral markers are being used and what is their purpose (Soper, 2023). This lack of transparency in K-12 settings is problematic because minors are less likely to understand the implications of continuous data tracking (Solove, 2006). To address this problem, adaptive learning platforms should implement students and parents data summaries that clearly outline what type of data is being collected and its purpose. In addition to that, the department of education should mandate schools to require age-appropriate consent mechanisms that distinguish between essential learning data and optional tracking features which will allow parents to make informed decisions on behalf of their children.

Once data is collected, it will be analyzed, categorized and used. In adaptive learning platforms, this information processing leads to profiling students to generate individualized lesson paths. In fact, i-Ready provides personalized lessons based on performance trends. Most of the time, students and parents are not fully aware of how these profiles are built or how it influences the content that students receive. This lack of clarity fits within Solove's privacy harm of exclusion in which users are denied meaningful access to the logic behind algorithmic decisions (Solove,2006). For example, students may be placed on remediation tracks based on the test interactions they had with the learning platform without human intervention to validate those algorithmic decisions. To increase transparency, platforms should publish simplified algorithmic impact statements that explain how personalized systems function and what indicators are used for decision-making. In addition to that, schools should audit how this classification is performed which could allow educators to supervise students' learning process.

Information dissemination privacy framework focuses on how the student data is shared beyond its original context. In the study case of Knewton, it partnered with content providers and used predictive analytics to improve learning outcomes. This system generates data logs that could be shared with third parties or used to train proprietary algorithms. Even though some of the sharing details are disclosed in privacy policies, it could go against the expectations of families who assume student data remains within the classroom (Solove,2006). Another example of data dissemination privacy harm is what would happen with this data if the company is sold to another one. To strengthen protections, schools should standardize the data sharing

agreements that restrict access to anonymized or aggregated data only and prohibit secondary use of it such as commercial product development marketing.

Per Solove's taxonomy, invasion of privacy addresses intrusive changes that affect user's autonomy. Adaptive learning platforms could adjust the pacing, level of difficulty, or content's sequence without informing the student. One example of this is DreamBox, it automatically increases the difficulty of problems based on the interactions without letting students know that their learning journey path shifted. Even though this can support differentiated learning, it could also undermine students' sense of control or lead to frustration if the changes are abrupt. Per Solove, this type of algorithmic personalization is an example of decisional interference as it subtly limits students' ability to make autonomous decisions (Solove,2006).

Nissenbaum

Nissenbaum's theory of contextual integrity focuses on whether the flow of information aligns with the norms of a specific social context, such as education. In the case of K-12 adaptive learning platforms, this framework becomes important when third-party vendors(DreamBox or i-Ready) collect and analyze student performance data that was traditionally shared only between teachers and school administrators. When this data is transmitted to external actors like software companies and analytics teams without clear consent from parents or students, it violates the expected flow of information within the classroom setting (Nissenbaum, 2010).

A key concern within contextual integrity is the repurposing of data. For example, student data collected to support learning outcomes may later be used for algorithm development or product improvement by the platform provider. Even if these uses are legal under FERPA or COPPA, they can still break the implicit trust families place in schools to safeguard educational data. To respect contextual norms, schools should require platforms to clearly define the purposes for which data is used and prohibit secondary uses that extend beyond instruction, such as internal R&D or commercial partnerships.

Mulligan

Mulligan's framework focuses on privacy harms caused by structural power imbalances and lack of agency in digital systems. In the case of adaptive learning platforms like i-Ready, students don't have a say in how their data is collected or how algorithmic decisions affect their learning. Even if parental consent is technically obtained, it's often hidden in lengthy Terms of Service with no meaningful alternatives, which make it more of a formality than a true choice (Mulligan et al., 2016). This reduces student autonomy and reinforces the idea that platform decisions are not to be questioned.

The imbalance of power is further seen in how decisions are embedded in vendor contracts and proprietary systems. Schools under pressure to implement tech solutions may end up adopting

platforms like DreamBox without understanding the full implications of its privacy trade-offs. These platforms hold more technical and legal leverage than school districts by giving providers control over how data is used and processed. To reduce this power imbalance, the department of education should negotiate stronger contracts and require platforms to offer clearer transparency tools and allow educators to override features.

Accountability gaps are also a major concern in Mulligan's framework (Mulligan et al., 2016). For example, if Knewton misidentifies a student's strengths and assigns inappropriate content, then it would be unclear whether the responsibility lies with the platform, school or teacher. As without defined lines of responsibility, parents will have little recourse to correct errors. In order to address this, schools should require platforms to provide clear documentation of how decisions are made and establish protocols for reviewing and correcting algorithmic mistakes. These steps would ensure that educational platforms respect not only privacy laws but also student dignity and fairness.

Privacy Policy Analysis

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a United States federal law that protects the privacy of students' data. For children under 18, FERPA grants guardians the right to access, correct, and control the disclosure of their children's education records and other personally identifiable information (PII). Schools must generally receive written consent from a student's guardian to release any information from a student's education record, with some exceptions for health and safety emergencies or for qualified "school officials."

FERPA establishes boundaries around data sharing and places a keen responsibility on schools to protect their students' data while requiring that third-party edtech vendors handling education records do so under strict confidentiality agreements, such as requiring guardian consent before disclosing PII. Additionally, FERPA provides a framework for schools to maintain oversight of edtech vendors, encouraging transparency and accountability in how student data is collected and used.

However, like many privacy policy regulations, FERPA was enacted before the rise of adaptive learning systems, and thus does not fully address the risks and complexities associated with real-time data collection, algorithmic profiling, or the automated decisions and recommendations that these systems make. FERPA primarily regulates access to and disclosure of education records without clearly defining or limiting how third-party learning system providers might utilize the data they collect. Additionally, and especially in an increasingly *privatized* educational environment, these edtech companies could be designated as "school officials," granting them access to student data without explicit informed guardian consent.

FERPA also lacks considerations for transparency in ensuring students' rights to fully understand algorithmic decisions and recommendations in regard to their education. DreamBox, for example, does not provide transparency in the data it collects, or how it uses that data to form further instruction, creating a gap in accountability and student autonomy.

COPPA

The Children's Online Privacy Protection Act (COPPA) is a United States federal law, which protects the privacy of children under the age of 13 online by giving parents control over what data is collected. Digital services (websites, apps) that collect data from children are required to receive guardian consent before doing so. These data collection services must be transparently disclosed, and parents must be allowed to review or delete their children's data.

While COPPA requires learning systems providers to obtain parental consent before collecting personal information from children under 13, it does not address how that data might be used after collection. This is highly important when considering adaptive learning environments,

which we know collect large amounts of complex data, continuously tracking and analyzing student behavior. COPPA also does not cover children over 13, leaving middle and high school students unprotected.

Most importantly, COPPA does not address algorithmic profiling, data retention, or the sharing of student data with third parties involved in the development or operation of similar adaptive systems, creating a significant gap in privacy coverage regulating how these tools could potentially shape long-term opportunities for students without transparency or actionable accountability.

GDPR

The General Data Protection Regulation (GDPR) is a comprehensive privacy law in the European Union, which provides specific protections for the online privacy of children under 16. Like COPPA, GDPR requires that data collecting entities obtain a guardian's consent before collecting personal data from a child, although several European countries have lowered this age requirement to 13. GDPR requires that privacy notices are written in clear, age-appropriate language, and gives children and their guardians the right to access, correct, and delete their data. Finally, it limits the use of children's data for profiling or marketing.

Ethical concerns with GDPR arise around profiling, potential biases in algorithmic decision-making, and longer-term impacts of data-driven learning paths on student development. For example, children may be encouraged to put less effort into educational tracks that they might find more enjoyment in but learn more slowly, in favor of subjects that they might find less interesting but have a natural knack for. Similarly, platforms dedicated to mathematics or other hard sciences, like DreamBox, may serve well for students adept at those subjects, while students with learning disabilities get left behind.

Further, due to the lack of transparency in the algorithms that these adaptive learning platforms use, schools may not fully understand or disclose the extent of data collection and use by their adaptive learning vendors. Because of this, parents will find it harder to work with their schools or ed-tech providers, or hold them accountable for poor learning outcomes or an otherwise unfulfilled child. Knewton, for example, does not grant access to how specific questions are answered, limiting both parents' and teachers' ability to understand students' responses and provide a truly personal and tailored learning experience.

Recommendations & Best Practices

To improve the effectiveness and security of adaptive learning platforms in K-12 settings, platforms should be required to provide transparent, user-friendly data summaries that clearly outline what type of data is collected, why it is collected, and how it supports personalized learning. This includes detailing what PII is gathered and how it is stored, as well as offering straightforward options for students and parents to remove data when desired. Additionally, platforms should include simplified algorithmic impact statements that explain how personalization works and how algorithmic decisions were made. These explanations should be accessible to both guardians and students, and should provide clarity on how the technology supports or influences learning outcomes.

At the policy level, the DOE should require platforms to implement age-appropriate consent mechanisms that distinguish between essential learning data and optional tracking features. This would empower guardians to make informed decisions on behalf of their students while safeguarding student privacy. The DOE should also push for stronger contracts that compel companies to offer transparency tools and grant educators the ability to override algorithmic decisions when necessary. Furthermore, schools should conduct regular audits of how platforms classify students and use data, allowing educators to monitor and support students' progress rather than relying solely on opaque system outputs.

Finally, adaptive learning platforms must support a holistic and inclusive learning environment. Systems should be designed to help students with learning challenges understand and manage their difficulties in a way that builds confidence and autonomy. This includes ensuring students progress at their own pace, even in shared classrooms, while still pursuing common learning goals. To cultivate passion and curiosity, platforms should include diverse subject matter, integrating the arts alongside core academic disciplines like science and math, supporting a more well-rounded and engaging educational experience.

Conclusions

Adaptive learning platforms may be promising for improving educational outcomes by providing personalized learning experiences. However, the ethical and legal challenges they present must not be overlooked. Our analysis shows several areas where improvements are needed to make sure these types of technologies are implemented responsibly in educational contexts.

In this paper, we explored how adaptive learning systems work and their impact on the learner experience. We analyzed issues around consent and privacy, using frameworks such as Nissenbaum's Contextual Integrity (Nissenbaum, 2010), and examined privacy risks through the lenses of Mulligan et al.'s (2015) Contextual Integrity and Solove's Taxonomy (Solove, 2006).

We analyzed these platforms within the context of several legal frameworks, FERPA, COPPA, and GDPR, to understand how well current regulations protect student data privacy and what gaps might exist. This legal analysis helped to assess the adequacy of existing consent mechanisms and privacy protections.

Throughout these analyses, we found several key themes:

1. **Student Data Collection and Consent Mechanisms:**
   Current consent mechanisms are often inadequate, lacking transparency and failing to provide students and parents with clear information about data collection practices. Adaptive learning platforms should adopt more robust and age-appropriate consent practices that clearly distinguish between essential and optional tracking features.
2. **Privacy Protections and Data Usage:**
   Privacy protections under existing frameworks like FERPA, COPPA, and GDPR are insufficient to address the complexities of real-time data collection and algorithmic profiling. Schools and platform providers (companies) need to establish stricter data governance policies and ensure that data usage aligns with only the intended educational purpose.
3. **Algorithmic Transparency and Fairness:**
   The lack of transparency in how adaptive algorithms make decisions could lead to issues like lack of accountability. Platforms should provide simplified algorithm impact statements and allow educators to audit and override the algorithm's decisions to maintain fairness and accountability.
4. **Ethical Considerations:**
   Ethical principles like informed consent, contextual integrity, and privacy harm should be integrated into the design and implementation of adaptive learning systems. This includes having a respect for the social context of education and addressing power imbalances between students, educators, and platform providers.

By addressing the recommendations outlined in this paper, adaptive learning systems could be used to have a positive impact on students' learning, in an ethical way.

Positionality Statements

Beth

My perspectives on this topic have been shaped by my upbringing in a predominantly white suburb of Detroit and my education in public K-12 schools and large, public universities. My academic background includes degrees in engineering and a PhD in science and mathematics education, which have influenced my understanding of the world through both technical and social science lenses. During my PhD in education, I conducted research on educational technology use in secondary science classrooms. My research also involved developing automated scoring models (using NLP and ML) for students' short response questions in science curriculum units. After my PhD, I have worked in education research, including as a learning scientist in an AI research lab on educational technology products.

My academic and professional background have allowed me to see both the drawback and potential benefits of using data analytics in educational technology. While I have made many attempts to understand the many needs of students and different learning paths, I myself have taken a very traditional path through my own education and rarely encountered difficulties in traditional schooling. Throughout the course of my professional career, I have worked on many facets of educational technology programs and conducted research in many different types of classrooms. I believe educational technology *can* provide a way for teachers to be more efficient and effective, but often these technologies are designed in ways that do not center student learning or the relationships in the classroom (teacher/student, student/peer).

Mayumy

My position in this research is shaped by my transnational educational journey. I completed my middle and high school education in Peru, where learning was rooted in traditional methods such as textbooks, handwritten assignments, and minimal exposure to digital tools. When I moved to the United States for college, I was introduced to adaptive learning platforms for the first time. The shift was striking because suddenly I had access to assignments, assessments, and course materials all in one click. As a first-time user of these interactive systems, I was focused on convenience and performance, with little awareness of the privacy implications or the extent of the data I was sharing.

Looking back, I now realize how little transparency there was in how these platforms operated. I didn't question what personal information was being collected or how it might be used beyond the classroom. This experience motivates my interest in critically evaluating the privacy and ethical dimensions of adaptive learning. I approach this topic as both a student who has

personally navigated these tools and a researcher who wants to ensure that future users, especially children, are better protected and more informed. I support educational systems that use technology responsibly and with the best interests of students in mind.

Jesse

I am a product of the public school system start-to-finish. Additionally, for more than a decade my mother worked for the Texas Education Agency developing early digital tools for curriculum design for teachers, and currently she works as a freelancer developing e-learning tools for large companies. I have never had to struggle in my educational career to learn English as a second language, and I have never been diagnosed with a learning disability.

This positive experience with a more traditional educational environment may lead me to have a slightly negative perspective in regard to the newest educational technologies. However, while I have a deep respect for teachers and their work, I also understand that technology can be a helpful tool for them to deliver their curriculum. At face value, adaptive learning systems seem like they may threaten the face-to-face interaction that is so valuable to both students and teachers. While this may indeed be the case, I also believe that it doesn't have to be. These tools should be developed and utilized in a responsible way that continues to not only encourage students to grow, but also forms social bonds between students and teachers, which may be more valuable than many other typical aspects of schooling.

Resources

Baker, R. S., & Hawn, A. (2022). Algorithmic bias in education. International journal of artificial intelligence in education, 1-41.

Baker, R. S., & Yacef, K. (2009). The state of educational data mining in 2009: A review and future visions. Journal of educational data mining, 1(1), 3-17.

Brusilovsky, P., & Millán, E. (2007). User models for adaptive hypermedia and adaptive educational systems. In The adaptive web: methods and strategies of web personalization (pp. 3-53). Berlin, Heidelberg: Springer Berlin Heidelberg.

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (1998). Retrieved from https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act

Curriculum Associates. (2025). About i-Ready. Retrieved from https://www.curriculumassociates.com/products/i-ready

Knewton. (2025). Getting to Know Knewton Alta and Mastery Learning. Retrieved from https://support.knewton.com/s/article/Getting-to-Know-Knewton-Alta-and-Mastery-Learning#:~:text=Educators%2C%20schools%20and%20universities%2C%20and,Knewton%20was%20founded%20in%202008.

Long, P., & Siemens, G. (2014). Penetrating the fog: analytics in learning and education. Italian Journal of Educational Technology, 22(3), 132-137.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160118.

National Center for Education Statistics. (2022). NAEP Long-Term Trend Assessment Results: Reading and Mathematics 2022. U.S. Department of Education. https://nces.ed.gov/nationsreportcard/

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Pane, J. F., Steiner, E. D., Baird, M. D., & Hamilton, L. S. (2015). Continued Progress: Promising Evidence on Personalized Learning. Rand Corporation.

Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477-560.

Soper, T. (2023, August 29). Seattle-area edtech company DreamBox Learning acquired by Discovery Education. GeekWire. Retrieved from https://www.geekwire.com/2023/seattle-area-edtech-company-dreambox-learning-acquired-by-discovery-education/

U.S. Department of Education. (2019). FERPA and the Pearson Data Breach. https://studentprivacy.ed.gov/resources/ferpa-and-pearson-data-breach