Published on *The National Law Review* https://natlawreview.com

The Development of AI and Protecting Student Data Privacy

Article By:

David P. Grosso

Michelle R. Bowling

Starshine S. Chun

Brooke M. Delaney

Educational technology (EdTech) has long been used by educators as a way to support teaching and facilitate student learning using a wide range of digital tools, platforms, and resources designed to engage students and encourage innovation. Generally, EdTech can include both products and services designed for the educational setting but can also include general-purpose technologies.

During the COVID-19 pandemic, schools were forced to pivot from in-person education to online learning, many using the billions of dollars of federal government pandemic aid to invest in EdTech, software, and other technology. EdTech's rapid adoption quickly became a growing concern for educators, students, and parents, often because the functionality of these tools and the data collected by them lack transparency, and general-use technologies that often lack the safeguards of those developed specifically for education use.

Although the benefits of these investments remain unclear, educators' appetite for EdTech continues to grow, especially for those that claim to harness the power of artificial intelligence (AI). While AI EdTech is not directly regulated by state or federal laws, K-12 school districts can mitigate the risk of adopting these tools by implementing policies for their evaluation, adoption, and implementation.

Understanding the Risk of AI in EdTech

Prior to adopting AI EdTech tools, educators should understand the potential risks of their use. For example, the data used to train AI's algorithms, especially when evaluating student work product, must be without bias. The rapid adoption of AI-based EdTech software in online learning bears risks that must be addressed, particularly when EdTech relies on open-source AI tools due to the potential

impact on children’s privacy and the security of those tools.

This discussion will be limited to two large risks of using AI EdTech: the security and privacy of student data, which may only be compounded through the use of open-source AI-based tools.

However, these issues are not unique to AI-based EdTech. Prior instances have shown that even non-AI EdTech tools can lead to significant breaches of student privacy and data security. Last year, the Federal Trade Commission (FTC) sued an online learning company, Edmodo, for collecting and using children’s data to target them with behavioral advertising. Security breaches in the EdTech sector have led to widespread data leaks. The security of online platforms, the protection of student data, and the prevention of unauthorized access are all issues that EdTech companies frequently face.

Current Children’s Privacy Landscape

While there are not laws that directly govern the intersection of AI and education, several laws and regulations indirectly touch upon this area, specifically in regulating data privacy. Notably, President Joe Biden's Executive Order from October 30, 2023, lays out a comprehensive strategy for the development and deployment of AI, which includes strict safety and security standards, a focus on privacy protection, and countermeasures against potential AI-induced discrimination. The order promotes the responsible use of AI in various sectors, including education and healthcare, and emphasizes international collaboration on AI matters.

As for current laws that indirectly regulate this area, federal regulations do offer some protections for pre-K to 12th grade students. The Children's Online Privacy Protection Act (COPPA) sets specific requirements for operators of websites or online services that knowingly collect personal data from children under 13. These operators must notify parents and secure their explicit consent before collecting, using, or disclosing a child's personal information. They must also ensure the safety of the collected information. However, a loophole allows schools to consent on behalf of parents if the education technology service provides the school with COPPA-mandated data collection notices and practices.

The FTC proposed codifying this loophole in a Notice of Proposed Rulemaking released on December 20, 2023. Other than a slight change in the proposed rule from the prior guidance, which is a new exception that allows parents to review collected data, refuse to permit operators' further use or future online collection of personal information, and to direct operators to delete such information, schools can continue to consent on behalf of students. Furthermore, COPPA falls short as it doesn't extend to teenagers and most websites don't verify users' ages, often leading to websites unknowingly interacting with minors. The inability to reliably obtain parental consent online presents another challenge. As a result, websites that comply with COPPA often resort to expensive offline verification methods or, in the worst-case scenario, disregard the regulation altogether.

Similarly, the Family Education Rights and Privacy Act (FERPA) was enacted to protect the privacy of student education records. It gives parents and students the right to access, amend, and control the disclosure of their education records. However, like COPPA, there are limitations. Private schools that do not receive funds are not protected under FERPA. FERPA does not prohibit the disclosure of directory information, such as the student’s name, address, and phone number unless the student or parent has opted out of such disclosure. Likewise, the Protection of Pupil Rights Act (PPRA) provides certain rights for parents of students such as student participation in surveys and use of personal information for marketing purposes. PPRA only applies to programs and activities funded by the US

Department of Education (ED), does not apply to the rights of students who are 18 years old or emancipated minors, and fails to address all aspects of student privacy such as the use of biometric data, online tracking, or data security.

However, some states, like California, are addressing the shortcomings in federal children's privacy policies through legislation such as AB 1584. This bill addresses some of the gaps in student privacy protection by authorizing local educational agencies to contract third-party services for digital storage, management, and retrieval of pupil records or to provide digital educational software, while enforcing strict regulations. It mandates that pupil records remain the property of the local educational agency and cannot be used by the third party for any purpose other than the requirements of the contract. Furthermore, it stipulates measures to ensure compliance with federal privacy acts and places the responsibility of notification on the third party in the event of unauthorized disclosure of the pupil's records.

Interestingly, although this bill was enacted prior to the widespread use of AI, its function can indirectly regulate AI systems. AI systems often require access to large amounts of data to function effectively. In the context of education, this could include student records, grades, and other personally identifiable information. AB 1584 provides a legal framework for how such data can be shared with third-party services, which could include AI service providers. Under AB 1584, schools can enter into contracts with AI service providers, allowing them to use student data for specific purposes like personalizing learning or improving educational outcomes. The law ensures that student data remains under the control of the local educational agency, and the AI provider must agree not to use the data for any purposes other than those specified in the agreement. AI providers also need to comply with the security and confidentiality provisions of AB 1584. They must implement measures to protect student data and notify the school if there's an unauthorized disclosure.

In the absence of a comprehensive federal privacy law, more than a dozen US states have taken it upon themselves to enact their own laws regulating the collection, use, and storage of residents' personal data. Notably, California has been a frontrunner in privacy legislation, passing the California Consumer Privacy Act (CCPA) in 2018. In January 2024, California introduced two new bills aimed at bolstering children's privacy rights. The Children's Data Privacy Act proposes amendments to the CCPA to strengthen protections for those under 18. It seeks to raise the age limit for affirmative authorization for data selling or sharing from 16 to 18. The California Privacy Protection Agency (CPPA) is also expected to establish an opt-out preference signal for those under 13 or 18 by July 2025. The second bill proposed is the Social Media Youth Addiction Law, which aims to regulate addictive features on social media platforms for users under 18. The bill defines "addictive feeds" as those where content is recommended based on a user's personal data or previous interactions. If passed, operators of such platforms would need parental consent or proof that the user isn't a minor to provide such feeds. Also, these platforms would be restricted from sending notifications to minor users during specific hours without parental consent.

The District of Columbia has also been a frontrunner in these efforts. In 2016, former DC Councilmember and now partner at ArentFox Schiff, David Grosso, successfully introduced and passed the Protecting Students Digital Privacy Act. The law requires an operator of an internet website, online service, online application, or mobile application used for pre-K-12 purposes to implement and maintain appropriate security measures to protect personally identifiable student information. It established procedures about accessing, analyzing, storing, or sharing that information, putting limits on an educational institution/vendor that provides a technological device to a student from accessing or tracking the device, and analyzing, selling, or sharing the activity or data. Further, the law prohibits a school from requiring or coercing a student to disclose the username or

password to a personal social media account, add school-based personnel to their list of contacts, or to change the settings that affect a third party’s ability to view the account.

Navigating AI EdTech Implementation as an Educator

As AI and EdTech increasingly integrate into education, they offer transformative enhancements to personalized learning and student engagement. However, this shift also brings complex challenges for educators. Navigating the intricacies of AI, including data privacy, algorithmic discrimination, and the implementation of these advanced technologies in a beneficial manner for students, can be daunting. Therefore, it's essential for educators to adopt a strategic and informed approach, ensuring they maximize the advantages of this evolving tech landscape while diligently preserving student privacy.

National Law Review, Volume XIV, Number 52