Hashed & Salted | A Privacy and Data Security Update
March 2022

AI in Ed Tech: Privacy considerations for AI-powered Ed Tech tools

Artificial intelligence (AI) is becoming more prevalent in educational technology (Ed Tech) tools. Since the pandemic, in particular, there has been an increase in demand for AI-powered tools that offer everything from personalized learning opportunities for students to school management resources for teachers, which can be leveraged regardless of whether the student is in person or remote. In general, AI tools rely on large data sets in order to achieve their desired purpose. While AI and its numerous applications may bring significant benefits, the very characteristics that make AI systems so powerful can also pose risks to individuals impacted by their use. For example, automated decision-making may replicate and amplify bias without the proper checks in place. AI also poses unique privacy considerations in the Ed Tech context because student data is often involved.

Here is a brief primer on AI in Ed Tech and a spotlight on what Ed Tech companies should consider when deploying AI technologies in Ed Tech tools.

What is AI?

AI is an umbrella term that refers to instances in which computers are accomplishing tasks that would otherwise require human intelligence. While this general term gets thrown around a lot, AI comes in quite a few different forms, ranging from simple automation to autonomous decision-making, which generally fall into two main categories:

- **Machine learning**. One particular subset of AI that garners a lot of attention is machine learning (ML). ML involves the use of algorithms that improve or "learn" through experience by going beyond carrying out the programmer's demands to adapt operations based on patterns gleaned from data. ML systems can be supervised (which involves data that has been labeled by humans), unsupervised (which involves the use of unlabeled data and exploiting connections that the computer identifies) or some combination of both.
- **Non-machine learning.** Not all AI involves ML. For example, symbolic AI—which relies on a human-supplied "knowledge base" to answer questions—is one type of AI that predated ML and is still in use today. This technology is not able to learn and adapt over time.

A great starting point for AI privacy compliance efforts is understanding the underlying technologies, because there may be unique considerations that are specific to the type of AI that is employed. For example, recommendations for how to approach the privacy principle of data minimization would likely vary, as non-ML systems are able to work with much smaller data sets to achieve its goals than ML systems, which generally require an immense amount of data to run.

Attorney Advertising

How are Ed Tech companies using AI, and what are the potential impacts?

With so much attention being given to the challenges and opportunities of AI use cases of the future—such as the promise of fully autonomous vehicles—it can be easy to inadvertently downplay the very real impacts of AI technologies that are already in use, including those that are integrated in students' lives. Children are increasingly interacting with AI in educational contexts. Common applications include:

- **Image recognition**. Image recognition is a system that has the ability to identify specific features of digital images and video. Schools that use facial recognition technology employ this application of AI, generally in the name of student safety. The use of this technology has been widely criticized, however, for normalizing a culture of surveillance in schools, among other criticisms. In fact, in light of increased scrutiny, New York became the first state to temporarily ban the use of facial recognition in schools (until July 2022) in order to give state education officials a chance to review facial recognition technology and the potential consequences of subjecting students to it.
- **Natural language processing (NLP)**. NLP is a functionality that enables machines to process, understand and/or generate audio and textual speech. When schools adopt apps to help students learn to read, such apps likely employ NLP. The intent behind the software is clearly to benefit students, but there can be unintended consequences. For example, students can be mislabeled if data is not accurately interpreted.
- **Predictive analytics**. Predictive analytics is the use of data analytics to predict trends, behavior patterns and outcomes. With the help of predictive analytics, AI can ensure that Ed Tech tools are personalized for individual students in order to keep them engaged and to better tailor school advising services to improve student outcomes. If there are issues with the data sets that are being analyzed or models that are used to analyze the data, however, the potential exists for bias, which can have long-lasting implications on a child's education and career trajectory.

The use cases above highlight just a few common examples of how AI is currently being used in education. It can be a powerful tool for transforming education in a positive way, as long as certain guardrails are in place.

How can Ed Tech companies manage privacy risks associated with AI?

Ed Tech companies can manage privacy risks associated with AI by considering the following:

- **Transparency and explainability**. Ed Tech companies should inform users when AI systems are being used and how those systems reach decisions. The Federal Trade Commission (FTC) has made it clear in its 2020 guidance on using AI and algorithms that companies will face enforcement action if they mislead consumers about their data practices, particularly when sensitive data is involved (including children's data, which the FTC regards as sensitive), even if that data is used to feed AI systems that are only running in the background. The FTC guidance also explicitly put companies on notice that they must be able to explain to consumers what data is being used and how algorithmic decisions are being made. The push for increased transparency and explainability doesn't stop here. Similar requirements are being introduced in new state laws like the California Privacy Rights Act (CPRA), which requires "meaningful information about logic" used in automated decision-making, and by large platforms like Apple, which requires privacy nutrition labels to help consumers understand how apps are using their data. As Ed Tech companies move forward with using AI-driven technologies, they should keep in mind that there are also risks associated with disclosing too much information. Companies must balance the need for transparency with the need to ensure that proprietary information is protected and that disclosures do not make AI systems more vulnerable to attack.
- **Data minimization**. Ed Tech companies should consider how they will address the privacy principle of data minimization. Data minimization refers to collecting only the data necessary to accomplish a specified purpose, and it is required under the European Union's General Data Protection Regulation (GDPR) as well as recently enacted privacy laws, including the CPRA, the Colorado Privacy Act (CPA) and Virginia's Consumer Data Protection Act (VCDPA). Data minimization can be challenging in the Ed Tech

space not only because AI relies on large amounts of data to work, but also because children may not understand the concept of privacy and may disclose more information than the product requires, particularly in instances where AI technology is embedded in toys or learning tools that process voice data. As a result, Ed Tech companies should carefully consider data retention periods and policies for disposing of any data that is not necessary for the product or service to function.

- **Fairness and nondiscrimination**. AI systems should be designed and used to maximize fairness and promote inclusivity. This is a challenge, as numerous reports have documented how AI systems may produce unfairly discriminatory outcomes due to (a) unconscious bias on the part of the AI model's designers, (b) the use of erroneous or inherently biased data, or (c) systemic errors in the algorithm itself. Increasingly, algorithmic impact assessments are being proposed to address these concerns and mitigate the risk of bias in AI. For example, the CPRA, VCDPA and CPA all contain provisions that make privacy risk assessments mandatory under certain circumstances. It's also worth noting that there is interest in addressing this issue specifically in the context of student privacy, as evidenced by a federal bill introduced by Rep. Lori Trahan, D-Mass., in July 2021, which would have required all Ed Tech companies that use "high-risk automated decision systems" in their products or services to provide detailed "technology impact assessments" directly to the FTC and to their customers via the publication of a modified version of the impact assessment on their website. Even though the bill did not pass last year, it may be reintroduced in 2022. More recently, at the state level, California Assembly members Buffy Wicks, D-Oakland, and Jordan Cunningham, R-Templeton, introduced a student privacy law that would also require risk assessments (among other things). Both the federal and state student privacy proposals draw inspiration from the U.K.'s Age Appropriate Design Code, which requires companies to consider the best interests of children when designing and deploying their products and services.
- **Restricted uses**. Last but not least, Ed Tech companies should remember that any data collected from students will likely come with use restrictions. This is due in large part to the Family Educational Privacy Rights Act (FERPA)—a federal law that applies to schools that receive federal funding—and its prohibition on disclosing personally identifiable information from students' education records to third parties without parental permission, unless an exception applies. Most data sharing between schools and Ed Tech companies falls under a very narrow exception that applies to Ed Tech companies that are essentially acting as a school official, and as such, only use data for educational purposes as specifically agreed to via contract. State student data privacy laws are often more restrictive than laws that govern children's and students' personal information at the federal level. Many of these laws prohibit Ed Tech companies from using student information for reasons other than "K-12 purposes," which is generally defined as purposes that are put in place at the direction of the school district for the benefit of the school. It is therefore unlikely that an Ed Tech company will be able to use the personal information collected from students to feed other AI systems under its corporate umbrella if those systems are powering products and services that are not intended for the school.

Conclusion

There have been increased calls for transparency, data minimization and risk assessments, as evidenced in privacy legislation and proposals at the federal and state levels that have been comprehensive and student-privacy specific. Ed Tech companies should begin to think about what they will need to do to comply with these requirements, even if they don't meet the minimum threshold under recently enacted state privacy legislation that would trigger compliance obligations. It seems unlikely that protecting student privacy will fall off of legislators' radar. It is no longer a question of whether increased privacy standards will be introduced in the student privacy space—instead the question is when.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Tanya Forsheit . . . . . tforsheit@loeb.com
Chanda Marlowe . . . . . cmarlowe@loeb.com

6899 01 REV1 03-16-2022