Reviewing 2024's Evolving EdTech Privacy Regulations

By **Amy Pimentel, Jessica Sawyer and John Ying** (January 15, 2025)

Amy Pimentel

Jessica Sawyer

John Ying

Use of educational technology, or EdTech — such as digital textbooks, instructional material and interactive applications — exploded during the COVID-19 pandemic, and these tools remain a key part of education.

Beyond student rosters and class enrollment data, these technologies gather survey results, measure study habits, and can even create psychological profiles to predict academic performance of classrooms and individual students. While these tools offer benefits like rapid feedback and personalized learning, they have the potential to create privacy risks for students and security risks for schools and educational companies alike.

Laws regulating the collection, use, disclosure and sharing of student data have not kept pace with recent technological advancements.

As a result, we've seen federal agencies like the Federal Trade Commission step into the gap between regulation and reality. These agencies have made clear that they intend to crack down on education technology companies if they illegally surveil or otherwise force parents and schools to trade their children's privacy rights to do schoolwork online or attend class remotely.[1]

This article provides a high-level summary of the state of privacy in the EdTech industry today, and highlights several key privacy and security issues that everyone in the education space should keep in mind while navigating this constantly shifting regulatory landscape.

State Supplements to FERPA

The Family Educational Rights and Privacy Act celebrated its 50th anniversary in 2024 and remains the primary federal privacy law regulating student data.[2] FERPA protects education records, i.e., records, files, documents and other materials that contain information directly related to a student and that are maintained by an educational agency or institution or a party acting on its behalf.[3]

FERPA aims to protect education records by limiting the circumstances under which they can be disclosed and requiring third parties — including EdTech vendors — to contractually agree to limit data use, implement robust security measures and take steps to protect student privacy. The law also grants rights to parents and eligible students to review, request corrections to and stop the release of their student records.

Over the years, a number of states have passed laws supplementing FERPA's protections. Most are based on California's Student Online Personal Information Protection Act, which, in part, prohibits EdTech apps and services targeting K-12 students from selling or using student personal information for targeted advertising or profiling.[4]

As classrooms increasingly rely on technology, states like Ohio, which amended its student

privacy law in 2024, are looking to maintain students' privacy protections, including by prohibiting technology providers from accessing or monitoring a school-issued device's location tracking features, recording features or student interactions, e.g. keystrokes and web browsing.[5]

Relatively new to the scene are the state comprehensive privacy laws, such as the California Consumer Privacy Act and the Colorado Privacy Act. While these laws generally exempt FERPA-regulated data, EdTech providers are likely to fall under the umbrella of these laws if they process sufficient data outside the scope of FERPA.

Since 2020, more than 20 states have enacted comprehensive privacy laws, with more to come in the next several years.

The Future of COPPA and KOSA

In early 2024, the FTC proposed amendments to the Children's Online Privacy Protection Act rule, aiming to strengthen children's privacy and put further limits on the ability to monetize children's data. COPPA applies to for-profit operators of commercial websites and online services that either directly target children under age 13 or knowingly collect personal information from children under 13.

COPPA follows a notice and consent model focused on parents. Before an online operator knowingly collects the personal information from someone under 13, it must first give notice to, and obtain verifiable consent from, the minor's parent or guardian.[6] The business must also, among other things, provide a clear and comprehensive privacy policy, honor the parent or guardian's rights to access and delete their child's personal information, and maintain the confidentiality, security and integrity of the information it collects.

The FTC's proposed rule changes included expanded requirements for providing privacy notices, obtaining parental consent, and ensuring data security and record retention, as well as updated obligations for COPPA safe harbor programs. There is a push to finalize the rule before the end of FTC Chairperson Lina Khan's term.[7] As children's privacy protections have wide bipartisan support, it is possible that the incoming FTC chair will make this a priority, too.

Meanwhile, in July, the U.S. Senate passed two new children's privacy acts: the Children and Teen's Online Privacy Protection Act, called COPPA 2.0, and the Kids Online Safety Act, or KOSA, with overwhelming bipartisan support.

COPPA 2.0 aims to modernize the decades-old law by expanding COPPA's protections to teens between 13 and 16 years old. It would also give parents of young minors and teens the types of data subject rights provided by state privacy laws, including rights to access, correct, modify or delete the minor's information.

KOSA, on the other hand, would raise the requirements for website privacy-by-default standards, require opt outs of personalized algorithmic recommendations, and increase parental controls over children's online activities. KOSA would also introduce risk audits and create liability for website operators for the content on websites aimed at minors and teens.

The status of COPPA 2.0 and KOSA remains murky. The U.S. House of Representatives' Committee on Energy and Commerce marked up the proposals in September, which resulted in a significantly different standard for the duty of care to safeguard children from harmful conduct. House Republicans moved forward with their version of the bill, which

would apply the duty of care only to large and impactful online companies with billions in revenue and millions of active users.

It remains to be seen whether these bills will continue to be a priority in the coming year, and whether the two chambers will reach an agreement on these foundational terms.

Key Privacy and Security Issues

It is clear that children's use of technology is in the spotlight, and EdTech privacy and security practices are an enforcement priority for not only the U.S. Congress and the FTC, but for state agencies and legislatures alike. As EdTech vendors develop products for schools, parents and other educational entities, we recommend keeping an eye on the following key issues.

Privacy of Student Data

Any company handling student data should carefully examine their privacy practices and aim to tailor the collection, use and sharing of student data to the extent necessary to provide the services. New services and data use should be carefully considered against privacy obligations.

EdTech vendors and schools should also provide transparency in privacy policies and COPPA notices. Both state student and comprehensive privacy laws may also have strict contracting, disclosure and data security requirements, which range in scope and effect from state to state.

EdTech Vendor Contracting

Contracts between schools and EdTech vendors should consider all privacy and security laws applicable to both parties and clearly state the data types that will be collected, used and disclosed as part of the services. Contracts should also include data processing terms that detail the processing activities, ownership rights or control over the data, any restrictions that must be placed on the data to protect student privacy, and data security practices that reasonably safeguard student data.

Further, we recommend incorporating terms addressing FERPA's "school official" exception — i.e., that the vendor performs an institutional service or function for which the institution would otherwise use employees, is under the direct control of the institution with respect to the use and maintenance of education records, and restricts certain uses and disclosures of personally identifiable information[8] — into contract templates to streamline the procurement process.

Security

Security is an important issue for all entities processing and maintaining student data. Some state laws, like Ohio S.B. 29, which became effective Oct. 24, require EdTech vendors to notify affected school districts of a data breach and to destroy or return all student records within 90 days of the contract's expiration.[9] We recommend EdTech vendors review their incident response procedures and data retention policies to ensure compliance.

Elements such as encryption at rest and in transit, multifactor authentication, employee training, and role-based access controls are all critical to fostering and maintaining trust with educational institutions. External audits and certifications based on industry standards

such as ISO 27001 or SOC2 can verify and improve existing cybersecurity processes. Mature cybersecurity practices and the associated certifications can also help lower cyberinsurance premiums by demonstrating robust controls and a lower risk profile.

Takeaways

The legal and regulatory landscape for EdTech is complex and ever-changing. Although the incoming Trump administration will likely bring a change in both the FTC chair[10] and the executive branch's stance on regulation, we expect states will expand to fill the open space, leveraging existing state laws and enforcement and passing new privacy and security legislation.

Amy Pimentel is a partner, Jessica Sawyer is counsel and John Ying is an associate at McDermott Will & Emery LLP.

[1] https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.

[2] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[3] Id.

[4] Cal. Bus. and Prof.s Code, ch. 22, § 22584 (b)(1) – (3).

[5] OH Rev. Code § 3319.325.

[6] 16 CFR § 312.4 (a) & (b).

[7] Tonya Riley and Cassandre Coyer, FTC Privacy Rules Will Be in Limbo Until Trump Transition, Bloomberg Law (Nov. 15, 2024) https://news.bloomberglaw.com/privacy-and-data-security/ftc-privacy-rules-to-endure-uncertainty-until-trump-transition.

[8] 34 CFR § 99.31 (a)(1)(i)(B)(1) – (3).

[9] Ohio General Assembly, SB29, § 3319.326 (B) & (C).

[10] https://www.law.com/nationallawjournal/2024/11/14/we-should-be-pragmatic-meet-the-possible-next-ftc-chair-/.