

Role for Federal Government in Safeguarding Student Data Privacy

**States Must Fill the Gaps**

by Khaliah Barnes

Today’s classrooms are equipped with Fitbits, tablets, mobile tracking apps, digital posters, and other technology to support classroom instruction. And some classes are conducted virtually so that all information is transferred digitally. Indeed, big data in the classroom has raised big problems for student privacy. Schools collect, digitize, and store sensitive student data on cloud-based services, creating a perfect storm in which student records are disclosed widely for many purposes without meaningful accountability.

Unsurprisingly, schools, companies, and others that have amassed student information have been unable to adequately safeguard it. They simply cannot keep up with all the data they have collected and have routinely experienced data breaches. These breaches have compromised grades, student financial information, Social Security numbers, and even special education records.

Congress charged the US Department of Education (ED) with enforcing the Family Educational Rights and Privacy Act (FERPA)—the main federal student privacy law—when it passed the law in 1974. Yet ED rarely investigates alleged FERPA violations or finds that schools have violated the law. Nor has the Federal Trade Commission, which has authority over the actions of private companies collecting student information, stepped in to investigate the behaviors of these companies. More can and should be done at both the state and federal levels to protect student privacy.

Congress should bolster federal baseline student privacy protections and not preempt states from enacting laws that provide additional protections.

**How Did We Get Here?**

FERPA grants students (and their parents) certain rights governing their records held by educational agencies and institutions receiving federal funding. Under FERPA, students may (1) access their education records maintained by the school; (2) amend erroneous records; and (3) subject to several exceptions, prohibit a school from disclosing their records without first obtaining their written consent.

Congress narrowly crafted these exceptions in FERPA to support school administration and other necessary and related school functions. Consequently, under FERPA’s written-disclosure exceptions, schools can disclose student records without student consent for several reasons: (1) to teachers, principals, and other “school officials” that require student records to perform “legitimate education interests”; (2) to other schools to which a student wants to enroll; (3) in connection with providing student financial aid; (4) for emergency purposes; (5) for school-sponsored research to enhance instruction; and (6) to evaluate and audit federally funded education programs.

In 2008 and 2011, however, ED proposed and implemented controversial rules that more broadly defined key FERPA terms to include entities, including private companies, outside the educational space. The Education Department’s rules fundamentally altered FERPA’s protections and student rights under the law. Under these rules, companies gained access to student records, and students and schools lost control over student data. My organization, the Electronic Privacy Information Center (EPIC), sued the department over its 2011 regulations. The case was eventually dismissed on procedural grounds, so...continued on pg 34
they even need to collect students’ personally identifiable information. Schools should work to implement privacy enhancing techniques, which minimize or eliminate the need to collect personally identifiable information. Such practices would permit schools to introduce innovative technology into the classroom without having to compromise student privacy. And privacy enhancing techniques, like anonymization, would permit states to achieve their goals of providing effective, equitable opportunities without putting student information at risk.

In 2014, EPIC created the Student Privacy Bill of Rights, an enforceable student privacy and data security framework. The Student Privacy Bill of Rights aims to put students back in control of their data by establishing six practices:

1. **Access and amendment.** Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.

2. **Focused collection.** Students have the right to reasonably limit student data that companies and schools collect and retain.

3. **Respect for context.** Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.

4. **Security.** Students have the right to secure and responsible data practices.

---

**Student Privacy Under Attack**

On a daily basis, students are required to turn over increasingly sensitive information. Here are just a few examples of the personal data—driven technology for instruction:

- Oral Roberts University requires all incoming students to wear Fitbit fitness trackers for a grade.

- Proctortrack, a popular remote proctoring service, scans students’ faces, picture IDs, and knuckles to verify student identification for remote test takers.

- GoGuardian permits teachers to monitor students’ classroom laptop screens in real time.
5. **Transparency.** Students have the right to clear and accessible information privacy and security practices.

6. **Accountability.** Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights.

As state boards grapple with the complexities of education technology, they should ask the important questions, execute privacy enhancing techniques, and implement the Student Privacy Bill of Rights. State boards and state education agencies can execute privacy enhancing techniques by collecting only aggregated student data. In addition, they should limit student data retention periods.

Moreover, state boards can evaluate whether their policies align with the Student Privacy Bill of Rights. They should ensure, for example, that students and parents have access to any information that states collect. State boards and state education agencies can make sure they are only using data for the original purposes for which they were collected. So if the state collects student data to implement a federal or state law, state boards must ensure that student data are not used for a secondary purpose.

State boards and other policymakers should keep in mind the maxim “If you can't protect it, don't collect it!”

States must be transparent regarding the types of information they collect, the purposes for which the information will be used, and to whom the information will be disclosed. Above all, state boards must implement accountability mechanisms when collecting student data. A state education chief privacy officer can field student and parent questions and provide oversight for state student privacy practices.

and administrators can turn to this person to evaluate new data-driven platforms, vendors, and policies. Parents can use this contact point to get clarity on privacy practices and protections, provide feedback on existing policies, and register concerns.

- **Train and enlist teachers and educators.**

As supported by a recent survey conducted by the Future of Privacy Forum, parents often trust individuals more than the “system.” Take advantage of this fact and encourage teachers to share the ways that data-driven technology helps students and makes their jobs easier.

- **Educate and engage students.**

Students are all too often left out of this discussion. Most are intensely curious to know about their progress and performance, especially relative to other classmates. While this information should be disseminated wisely to avoid social stigma and self-fulfilling prophecies, a little self-knowledge can go a long way in both motivating students and informing them about the data that are shaping not only their education but much of their lives.

While much of this advice may seem like common sense, it is difficult to integrate these ideas into daily institutional practices, given other pressing needs and the tension surrounding student privacy conversations. Consideration, communication, and proactive policies will not magically erase these differences, but they are a prerequisite for more constructive conversations that further the objective on which everyone does agree: an education system that does its best to support student success.

---


---

Elana Zeide is an attorney, consultant, and Fellow at New York University’s Information Law Institute.
Nearly all education stakeholders can agree on two things. First, using data to personalize learning for all students is the wave of the future and not a fad. Second, safeguarding student data privacy is both critical and urgent.

Happily, the two are not mutually exclusive. Districts, states, and the federal government have a role to play in both ensuring the privacy and security of students’ personal information on the one hand and, on the other, in building trust that student data are used appropriately. In fact, privacy safeguards and effective data use are mutually supportive. Strong safeguards enable schools to confidently make the case to parents that student data are being used safely in beneficial ways.

Trust Matters

Education data can benefit everyone. Educators have richer, more useful information than ever before to tailor their practices to students’ individual needs. Parents can make better informed decisions about their children’s learning. Students can better manage their progress toward their college and career goals. But they will not use data they don’t trust or in an environment that doesn’t value that trust. The immense potential of student data is thwarted when parents, teachers, and school leaders do not have confidence that student information is reliable, safe, and secure.

States and districts can build trust in student data by providing value to parents and teachers (e.g., How does sharing this information benefit my student?) and by being utterly transparent about their policies and procedures (e.g., What data are collected and why? Who has access? How are data shared? What privacy safeguards are in place?). While laws are essential, you can't legislate trust. It must be built.

A Patchwork of Privacy Laws

Equally as important as building trust is building a strong legal foundation for protecting student privacy. All levels of government—local, state, and federal—are responsible. Rising to the challenge, states have begun legislating around student data privacy. In 2015 alone, legislatures in 47 states introduced 188 bills. States have demonstrated impressive leadership. However, the results are a mixed bag.

State efforts have increased transparency about what data are collected and for what purposes, stronger privacy security laws and policies, clearer governance of data, and more open communication across the field—especially with parents and teachers. At the same time, several states have introduced or passed legislation that would (often unintentionally) limit the use of student data to improve learning and create an undue burden for teachers and administrators, often without actually enacting any significant data protections.

This patchwork of state laws creates an opportunity for the federal government to think critically about its role in safeguarding student privacy. The federal government can be a critical partner in complementing, supporting, and reinforcing state efforts to protect student information. Existing federal laws—including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children’s Online Privacy Protection Act (COPPA)—offer an important but incomplete legal foundation (as detailed in Elana Zeide’s article on page 21). The federal government should consider how their own patchwork of privacy laws can be amended and implemented better. Ultimately, states and the federal government ought to work together to develop a more streamlined system of legal protection.
A Role for the Feds

Information practices and technological capabilities are light-years ahead of what they were when current federal privacy laws were enacted. Federal action should continue to align and clarify student protections while working to advance the field’s capacity to protect student information. My organization, Data Quality Campaign, has identified three roles we believe the federal government should play in safeguarding student data privacy.

Legislating for the Future. The integration of technology into education has significant implications for the privacy and security of student information, and federal laws haven’t caught up. Student data are now collected, stored, and shared digitally, often in cloud-based systems. While COPPA addresses online privacy, it is not always clear to school districts and educators how the law applies to use of online service providers and applications. And while FERPA has been applied to electronic records in some situations, the law is not designed to cover data collected outside of a student’s official school record. Neither law sufficiently addresses current and potential security concerns related to evolving digital learning environments.

Federal law must be strong enough to protect student information in an increasingly digital school environment yet broad enough to allow states and districts to innovate. Changes to FERPA should recognize the digital environments in which student data are generated and stored, account for schools’ uses of third-party online applications that collect student information, and address the need for security safeguards designed for modern digital environments.

Cross-Agency Coordination and Clarity. States and districts must navigate the protections offered by federal laws: FERPA and PPRA, which are administered by the US Department of Education (ED), and COPPA, which is administered by the Federal Trade Commission (FTC). By coordinating across agencies to provide clarity to those on the ground as to how these different privacy laws work together, the federal government can make this navigation easier. When the federal government provides consistent definitions and standards, states and districts can better understand and build upon this foundation to protect student information.

In particular, ED and the FTC can issue joint guidance to help states and districts implement federal privacy laws and better inform state laws and policies. They can help clarify for the public which federal laws govern student data privacy, their application in school settings, and federal governance of websites and online applications.

Support States and Districts. Individuals in districts and schools need training and support to build a culture of trust and implement best practices in data privacy and security, and the federal government already has begun to develop some tools to support local infrastructure and capacity building. The Privacy Technical Assistance Center (PTAC), for example, offers a hotline and guidance on issues such as data breach response and model terms of service. But more is needed.

Continued federal attention to the role of states and districts in safeguarding student data is vital. The federal government can support them by providing more tools and resources to help them adopt policies and best practices in transparency, governance, and privacy and security. These supports can also include funding for building capacity—especially through related training and professional development—throughout the system, from the state to the local, school, and classroom levels. The newly minted Every Student Succeeds Act (ESSA) takes a step in the right direction by explicitly listing data literacy and data privacy trainings as allowable uses of professional development grant (Title II) funds for states and districts.

Moving Forward

Federal leadership in student data privacy can reduce the burden on states by aligning and clarifying the current patchwork of federal laws and by helping advance the education sector’s capacity to protect student information. Given the upcoming implementation of ESSA and a recent focus on this issue by members of Congress and the White House, there is a unique opportunity for federal action. A solid legal foundation at the federal level clears the path for states and districts to take on the hard work of fostering trust around education data use. When parents, teachers, and school leaders trust that the information is reliable, secure, and protected—and is being used in an environment that values their trust—then the immense potential of education data to improve student learning can be unleashed.