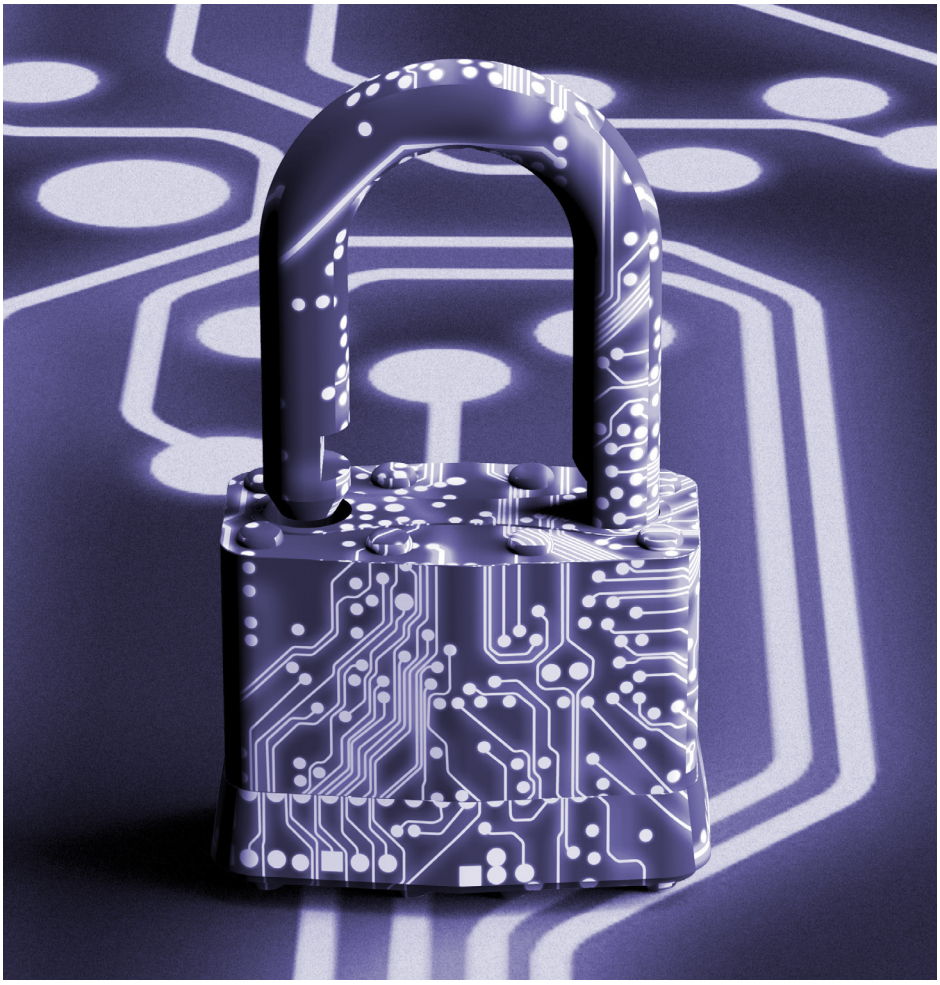

Student Data Privacy:
Going Beyond Compliance

Addressing parents' fears that student data will be abused requires states to shift toward proactive management of education records.

by Elana Zeide

With Edward Snowden's 2013 revelations about surveillance by the National Security Agency, privacy once again became a hot topic in public debate, but this time in a world increasingly mediated by digital tools. The debate quickly extended beyond broad consumer and citizen concerns to focus on student data privacy. Since 2013, most states have considered one or more bills to protect student data, with many giving state boards of education more authority in this arena. The best of this legislation goes beyond compliance to better address stakeholders' fears.

States that take this approach have adopted two key practices in implementation of new state laws: They develop a comprehensive understanding of what information state and local education agencies (SEAs and LEAs) hold, and they communicate clearly with parents about what happens to student data, how these data are protected, and how data collections benefit students.

Technology Moves ahead of Policy

Anchored by the Family Educational Rights and Privacy Act (FERPA), the existing student data regulatory system satisfied stakeholders for almost 40 years in part because of the inherent limitations in how paper-based student records could be shared, used, and repurposed.

Federal law has not kept pace with the technological advances that have transformed education data collection,

storage, and use. Cloud storage allows seamless information sharing at minimal cost. Big data tools can extract patterns and insights from aggregated data in ways that benefit not only students, but also educational institutions, corporations, and policymakers. As in other contexts, all these information users are focusing on using data as "evidence" to drive decision making, often through algorithmic analysis and predictive modeling.

Fears abound. Parents worry that this widened access to school data will jeopardize their children's safety or be leveraged by companies for profit. Educators fear that student information will be turned against them as accountability metrics. Privacy and civil rights advocates fear that data-driven decision making may retrench, rather than redress, existing inequalities.

Separating privacy from broader education policy is essential for state boards that wish to have constructive conversations with diverse stakeholders.

No Consensus on Privacy Practices

Everyone seems to agree that student privacy should be better protected. There is no real consensus and many different ideas about how education institutions and agencies should do it. Some practices seek to regulate schools; others focus on operators of school-directed services. Some restrict the type of data that can be collected, dictate how they are protected, and restrict their use. Many focus on the role of noneducational actors that receive information from educational institutions and agencies, prohibiting them from selling this data or using it to drive targeted marketing.

With constantly evolving technology, cultural norms, and regulatory landscapes, it is no wonder there is no broad consensus regarding how best to protect student privacy. The situation places education institutions and agencies in the difficult position of creating rules in a dynamic environment to meet the sometimes countervailing needs of stakeholders.

Conflating Education Policy with Privacy Practices

The wealth of student information became increasingly available just as controversial education policies were being set that rely on quantitative data to assess student performance, provide accountability metrics, and inform policymaking. Consequently, it is easy to conflate policy debates about how data ought to be used and privacy-focused questions about how such information should be handled in education environments. As a result, many arguments for "student privacy" in fact revolve around opposition to data-reliant education policies such as adoption of the Common Core and not specific information-handling practices in schools and classrooms.

Separating privacy from broader education policy is essential for state boards that wish to have constructive conversations with diverse stakeholders. It is important to remember—and to remind others—of this distinction. Privacy involves practices governing the sharing, use, protection, and retention of personal information. Because digital platforms have become integral to all aspects of society, it is fair to say that schools, districts, and state educational agencies will still have access to a significant amount of student information even in the absence of data-driven education policies. Educators and administrators will still need to ensure that appropriate rules and policies are put in place to protect student data regardless of its broader role in the education system.

Other Concerns

Safety and Security. Another set of issues involves preventing unauthorized data access, which the ease of information flows through and outside school networks make possible. Parents worry that school data collection will provide information to would-be predators, and they fear that data breaches will lead to identity theft.

Commercial Exploitation. Much of the student privacy debate concerns the individuals and entities with which schools share personally identifiable student information. As discussed above, FERPA limits school disclosure to some extent but doesn't address the ways that entities can now repurpose information collected in the course of providing schools educational services. Parents wonder if these secondary uses will be used to conduct experiments or generate profit and what the effect might be on students.

Unintentional Effects of Educational Use. Parents fear that information monitored by schools in the name of security and bullying prevention will be used against students. Stakeholders worry that data collected by educational actors will become digital dossiers, the modern-day equivalents of the proverbial

permanent record, and foreclose students' future opportunities because of early mistakes or missteps. They fear the repercussions of information sharing even within institutions. They wonder if historical performance data will become self-fulfilling prophecy.

FERPA's Flaws

Traditional student privacy regulatory frameworks like FERPA do not adequately address all of these concerns. FERPA's fundamental structure was built in an era of paper records and is a poor match for today's concerns. Consequently, it is difficult to interpret and apply the statute to today's technology. FERPA also fails to address important issues that arise from technological advances. So while the federal law should expand technical definitions and the scope of protection around personally identifiable information, such updates would only touch the surface of current concerns.

More important, in its focus on disclosure, FERPA doesn't address educational actors' own information practices. Because it delegates the bulk of data-related decision making to educational institutions without strong, accompanying transparency requirements and accountability mechanisms, FERPA cannot ease stakeholders' fears.

FERPA's transparency obligations are minimal, requiring only that educational actors provide student and parents with access to personally identifiable student information. Under the school official exception in annual FERPA notices, schools and districts must also include information about their nonconsensual disclosure policies, but these notices tend to be so broad as to provide little concrete information about the data schools collect and share and the purposes this collection and sharing serves.

The same is true of information use on the agency level. The Department of Education revised FERPA's regulations in 2008 and 2011 to better accommodate the reality of digitized records and networked information flow by creating explicit rules allowing SEAs to share personally identifiable student data more easily with researchers and vendors managing state longitudinal data systems. These regulations use contractual provisions, instead of requiring "direct control," to ensure recipients protect and use covered information appropriately. Many advocates and parents are not aware of what concrete limitations these contracts impose.

Schools, LEAs, and SEAs must also provide parents with the opportunity to challenge student data. Given the quantity, granularity, and dispersal of collected student information, however, it is difficult to do so in a meaningful manner.

Another important FERPA feature is its compliance orientation. While experts often speak of FERPA as permitting this or prohibiting that, it is technically a statute that conditions federal funding on compliance with its provisions. The consequence for noncompliance is withdrawal of federal funding. However, given the drastic nature of that measure and the way that might ultimately harm the very students the statute seeks to protect, the US Department of Education administers FERPA with an eye toward encouraging compliance rather than punishing noncompliance.

Education institutions and agencies must demonstrate a policy or practice of consistent violations before they will be sanctioned. In effect, education actors get benefit of the doubt. The statute presumes that they will comply to the best of their ability and that this effort will be enough to prevent harm. Stakeholders may not operate with the same faith.

In the absence of rigorous institutional transparency, stakeholders have almost no sense of, as well as no say in, the information practices related to student data. Without a clear understanding of schools' privacy practices and no evidence of consequences for information misuse or mismanagement, stakeholders may get a sense that schools are not being diligent about how they protect and use student data. This understandably creates a sense of unease.

Stakeholders are neither Luddites nor helicopter parents. Given the fast pace of technological development and new analytical tools that reveal increasing amounts of information and can be applied to more and more uses beyond their original application, it is impossible to predict what data collected today will reveal tomorrow and how those data will be used. It is logical to hesitate in the face of such uncertainty, especially in the absence of a sense of transparency or accountability accompanying these tools and technology.

Beyond Compliance

FERPA governs education agencies' disclosures to outsiders but does not restrict their own practices regarding data collection, use, protection, and retention. This fact, coupled with its limited minimal transparency obligations and reticence about enforcement contribute to stakeholder resistance. It is only natural to fear that which is unknown and over which one has no control. Accordingly, I advise individuals and entities with access to personal student information to go beyond mere compliance toward proactive management of information and privacy. Adopting and articulating public policies can go a long away in reassuring parents that education agencies are thoughtful stewards of student information.

Adopting and articulating public policies can go a long way in reassuring parents that education agencies are thoughtful stewards of student information.

Because education technology offers such promise, proponents often lose sight of the fears it prompts. When proponents speak of the benefits of putting data-driven technologies in place, the message may not resonate with parents, who are concerned with the effects on individual students in the present rather than those in the future or the education system as a whole. State longitudinal data systems, for example, have not been promoted as ways to improve the immediate educational quality or opportunities of students today. Viewed from that perspective, parents' hesitation makes eminent sense: Why put a child at potential risk for rewards that she won't reap?

A Three-Tier System

I find it helps for policymakers to view proposed information practices and privacy policies through a three-tier framework when crafting contracts, more information privacy rules, and communicating with educators and stakeholders. First, examine practices from the perspective of a student data subject or his parent. Second, consider the ramifications of new technologies and policies on students collectively. Third, examine how information use promotes extra-educational goals such as research and profit making. Understanding these separate strands may not assuage all stakeholders, but it will prepare education agencies to respond to pushback against new technology and information practices.

Best Practices

Inventory and Transparency. In the absence of control over their child's data, parents need information about what is happening to feel secure. Stakeholders may interpret the lack of readily available information or transparency not as reticence or omission but as deliberate deception.

Transparency first requires a thorough inventory of the data a school or education agency collects, the paths through which it flows, and the rules that govern it. Ideally, education agencies would then publish what information they collect and why, how it is used, who can access it, and how it is protected.

Very few schools, districts, or states have this level of transparency. And they likely would find the idea daunting: No one wants to trigger a backlash. However, openness will ultimately foster trust. Detailed transparency may be challenging at first, but such an investment in establishing community and stakeholder trust is worth it.

Privacy Policies and Principles. Given the amount of detail involved and the pace at which it changes, it is best to begin by articulating broad approaches to data—principles such as data minimization or restrictions on commercial repurposing. For example, schools should create explicit rules regarding employee data-sharing authority and accountability, including policies covering adoption of data-sharing technologies in classrooms that frequently do not require administrative approval. By setting out practices and privacy policies beforehand, schools and education agencies will likely receive the benefit of the doubt.

Another helpful tactic is to communicate the need for information practices to be standardized. It may be difficult for those outside the school system to understand the confusion that would be caused if parent preferences dictated data flow for every decision.

- **Designate a privacy point person or position.** Many states have created chief privacy officer positions to be this point person. Even if decision-making authority is more broadly dispersed, there should be a specific place where stakeholders can turn for privacy guidance and clarification. Teachers

...continued on pg 35

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. ■

[1]See, for example, University of Maryland, "UMD Data Breach," http://www.umd.edu/datasecurity/; DC Office of the State Superintendent for Education, "Data Disclosure Notice," http://osse.dc.gov/release/data-disclosure-notice.
[2]EPIC, "Department of Ed FERPA Enforcement FOIA Request," October 15, 2014, https://epic.org/foia/ed/ferpa/.

continued from pg 24...Student Data Privacy: Going Beyond Compliance

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.