“Why a ‘Student Privacy Bill of Rights’ Is Desperately Needed”

By Khaliah Barnes  
*Washington Post*  
March 6, 2014

As schools increasingly use educational technology (“EdTech”) and other cloud-based services, students are tracked, traced, monitored, and scored now more than ever before. While this technology may present some advantages, it also substantially raises the risks to student privacy. Over the past several months, protecting student privacy and safeguarding student data have been hot topics in education policy. Student privacy has continued to garner attention from both Congress and states. Amid the debates on how to best protect student privacy while using advanced technology, one thing remains clear: it’s time for students to regain control of their information. After all, this information has lasting impacts on their futures. It’s time for a student privacy bill of rights.

I recently had the pleasure of participating in a student privacy summit hosted by Common Sense Media and the Annenberg Retreat at Sunnylands. The summit convened many of the key stakeholders in education privacy, including the Secretary of Education Arne Duncan, Massachusetts Sen. Ed Markey, Federal Trade Commission member Julie Brill, and others including parents, professors, superintendents, policymakers, technologists, industry representatives, and journalists. Noticeably, we did not hear from actual students as we grappled with the ever-growing complexities of collecting and protecting student data. (Granted it was in the middle of a school day, but if ever a hall pass was warranted, the student privacy summit would be the perfect reason). We addressed an array of issues surrounding student privacy, from the type of data that schools and their private vendors collect, to different EdTech approaches in big cities and rural towns, to the conflicting jurisdictional issues between the FTC and the Education Department.

The summit dialogue revealed that federal student privacy laws—the *Family Educational Rights and Privacy Act* (“FERPA”) and the *Protection of Pupil Rights Amendment* (“PPRA”)— do not apply to a lot of the student data that schools and private companies amass. Because of this, there was a general consensus on the need for a modern student privacy and data protection framework. Some called for a badge mechanism, whereby companies that uphold student privacy would receive a “seal of approval” signaling their commitment to protecting student information. The Software & Information Industry Association (“SIIA”), announced its proposed framework, “Industry Best Practices to Safeguard Student Information Privacy and Data Security and Advance the Effective Use of Technology in Education.”

These industry practices reflect much of the status quo, which does very little to actually safeguard student privacy and information. For example, SIIA’s best practices don’t allow students to access and amend their information that private vendors collect. As I discussed during my summit remarks, the ability for student to access and amend their records is a due process issue. They should be able to redress erroneous, misleading, or embarrassing records that private companies compile. The practices also don’t address student data deletion and retention policies. Better practices would permit students to delete their information after it has been used for its initial and primary education purpose. Additionally, there’s no enforcement mechanism for these practices. Companies are simply not accountable to schools and students, especially because federal and state student privacy laws do not apply to most student data that industry service providers collect.
The Education Department also announced its suggested framework for protecting student privacy, the highly anticipated “Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices.” Unfortunately, the document raises more questions than answers. Indeed, the Education Department’s answer to “Is student information used in online educational services protected by FERPA?” is “It depends.” This is alarming because it is the Education Department’s regulations that permit private companies to access education records. But the Department’s guidance illustrates how little privacy protection students now have pursuant to those regulations. As a baseline matter, the guidance acknowledges that federal student privacy laws may not apply to certain student information that private companies collect and maintain. The guidance details that in many situations, regulations do not even require schools to have written agreements when disclosing student information to private EdTech companies. The guidance also explains that federal law does not prohibit school email providers from serving “generalized, non-targeted advertisements” to students via email or other online services.

Among other things, the Education Department recommends that schools contracting with EdTech providers print and save terms of service from click-wrap agreements; define the purposes for which providers may use student data; and specify “whether the data collected belongs to the school/district or the provider.” The Education Department should amend these recommendations and clarify that the data doesn’t belong to the school or the provider, but rather the student (or eligible parent). This is critical, because with ownership comes control. When students own their information, they have an active role in protecting their data.

We need to put students back in control of their data, the way FERPA and the PPRA imagined. Students didn’t participate in the student privacy summit or in the crafting of the aforementioned best practices, but students should participate in reclaiming their privacy rights. And that’s why it’s time for a Student Privacy Bill of Rights. These aren’t contract principles or aspirational promises, but rather a framework of enforceable rights.

In line with the president’s Consumer Privacy Bill of Rights, which is based largely based on the well-established Fair Information Practices (“FIPs”), schools, districts, and EdTech and other cloud-based service providers should adhere to the following practices when collecting student data. These rights should transfer from parents or legal guardians to students once the student is 18 years old or attending college.

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.

   There are gaps in current laws and proposed frameworks concerning students’ access and amendment to their data. Schools, companies, government agencies, and other entities that collect any student information should provide student access to this information. This includes access to any automated decision-making rule-based systems (i.e, personalized learning algorithms) and behavioral information.

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

   EdTech companies should collect only as much student data as they need to complete specified purposes. “Educational purposes” and “educational quality” are frequent examples of broad and fluid purposes that grant EdTech carte blanche to collect troves of student data. A more focused collection
would, for example, specify that the collection is necessary to “improve fifth grade reading skills” or “enhance college-level physics courses.” In focusing student data collection for specific purposes, schools and companies should consider the sensitivity of the data and the associated privacy risks.

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.

Schools and companies should never repurpose student data without express written student consent. This includes using student data to serve generalized or targeted advertisements. The Education Department’s guidance states that federal student privacy laws do no prohibit schools or districts “from allowing a provider acting as a school official from serving ads to all students in email or other online services.” This allows service providers to repurpose the information. Schools provide private companies access to student data to help enhance education quality. When companies use this access for general marketing purposes, they have repurposed the student data and turned the classroom into a marketplace.

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

Amid recent, large-scale student data breaches, schools and companies must increase their data safeguards to ward against “unauthorized access, use, destruction, or modification; and improper disclosure” as described in the CPBR. Companies should immediately notify schools, students, and appropriate law enforcement of any breach. And schools should immediately notify students when there is a breach. Schools should refrain from collecting information if they cannot adequately protect it. Securing student information also entails deleting and de-identifying information after it has been used for its initial and primary purposes (no secondary uses allowed!).

5. Transparency: Students have the right to clear and accessible information privacy and security practices

Schools and companies should publish the types of information they collect, the purposes for which the information will be used, and the security practices in place. Schools and companies should also publish algorithms behind their decision-making.

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

Schools and companies should be accountable to enforcement authorities and students for violating these practices.

The Student Privacy Bill of Rights puts students back in control of their data and provides the privacy, security, and due process protections that students deserve.