



Sheila Kaplan
3 Pierrepont Pl.
Brooklyn, NY 11201
347-486-0361
www.educationnewyork.com
sheila@educationnewyork.com

Education NEW YORK

FERPA, COMMON CORE STATE STANDARDS & DATA-SHARING

As the 45 states that have adopted Common Core Standards begin implementation serious concerns are being raised about the impact on the privacy of students and their families.

The federal Family Educational Rights Privacy Act, or FERPA, was enacted in 1974 to protect the privacy of education records and directory information, which includes name, address, phone number, date of birth, and e-mail address, among other personally identifiable information.

Schools are a rich source of personal information about children that can be legally and illegally accessed by third parties. With incidences of identity theft, database hacking, and sale of personal information rampant, there is an urgent need to protect students' rights under FERPA and raise awareness of aspects of the law that may compromise the privacy of students and their families.

In 2008 and 2011, amendments to FERPA gave third parties, including private companies, increased access to student data. It is significant that in 2008, the amendments to FERPA expanded the definitions of "school officials" who have access to student data to include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform." This change has the effect of increasing the market for student data.

For example, the amendments give companies like Google and Parchment access to education records and other private student information. As the Electronic Privacy Information Center (EPIC) points out: "Students are paying the cost to use Google's 'free' servers by providing access to their sensitive data and communications."

The 2011 amendments allow the release of student records for non-academic purposes and undermine parental consent provisions. The changes also promote the public use of student IDs that enable access to private educational records.

These amendments are critical to supporting initiatives like Common Core that depend on collection of student data to monitor implementation and measure success. Schools across the country will contract with third-party vendors to provide products, programs, and services in order to meet the Common Core requirements -- and government agencies and researchers will be mining student information for studies and databases. The FERPA amendments are paving the way toward greater accessibility to student data while providing no meaningful sanctions or protections against breaches of student privacy. As amended, FERPA will loosen privacy protections while helping to promote the business of education.

How can we stop this invasion of student and family privacy in the name of education reform?

EPIC is one national group that is sounding the alarm on these changes to FERPA. EPIC filed suit against the U.S. Department of Education claiming that the Department lacks the statutory authority to amend FERPA to make student data more available and accessible to third parties -- effectively changing the privacy law. *EPIC vs. Department of Education* is pending in federal district court in Washington, D.C.

In bringing suit EPIC mentions the numerous education organizations as well as private citizens who submitted comments *against* the changes during the Department's public comment period in 2011. They included the American Council on Education. ACE stated that: "We believe the proposed regulations unravel student privacy protections in significant ways that are inconsistent with congressional intent."

The comment by ACE was echoed by other influential groups, including the American Civil Liberties Union, the Privacy Rights Clearinghouse, the Center on Law and Information Policy at Fordham University Law School, and the World Privacy Forum, which stated that "Student and parental records will be scattered to the winds to remote and untraceable parties, used improperly, maintained with insufficient security, and become fodder for marketers, hackers, and criminals. The confidentiality that FERPA promised to students and their families will be lost."

The American Association of Collegiate Registrars and Admissions Officers also raised a number of concerns about the changes, charging that "The proposed regulations have been overwhelmingly influenced by the single-issue lobbying of a well-financed campaign to promote a data free-for-all in the name of educational reform."

It is important to note the interests of those who submitted comments in favor of the FERPA amendments. For example, the Software & Information Industry Association, which represents more than 500 leading high-tech companies, argues in favor of easier access for vendors to student data. The College Board supported the amendments because they facilitate “the robust educational research and evaluation needed to improve opportunities and outcomes for all students along the P-16 continuum.” This means the College Board would have greater access to student data to, in their words, “validate our tests, assessments, and educational programs” -- their primary business.

The Education Information Management Advisory Consortium of the Council of Chief State School Officers noted that the FERPA changes will “allow us to facilitate better research and evaluation using our statewide longitudinal data systems.” And the Western Interstate Commission for Higher Education supported easier access to student data to develop a multi-state longitudinal data exchange that incorporates secondary and post-secondary education data and workforce data. This project is supported by the Gates Foundation.

Note that protecting the privacy of student information is not the primary concern of those commenting in favor of the amendments.

What lies ahead for student privacy when private companies, government agencies, and a wide range of researchers have greater access to student data and information? I mentioned earlier the “business of education.” This phrase was used by the Council of Chief State School Officers in their comment in support of FERPA changes. Business is booming and groups like CCSSO are benefiting. Technology startups aimed at K-12 schools attracted more than \$425 million in venture capital last year.

CCSSO initiated the creation of a \$100 million database with funds from the Gates Foundation to track public school students’ information and academic records from kindergarten through high school. This is called the Shared Learning Infrastructure and it is now being run by an organization called inBloom, specifically created to operate the system.

The SLI will collect and maintain a range of student data in two “buckets” -- the first will include names, demographic information, discipline history, grade, test results, attendance, standards mastered--the list goes on. While schools may already have much of this data, this information is not usually stored in one place.

The second “bucket” will store information about instructional content and materials that will be linked to student test data in the SLI. Using Learning Resource Metadata Initiative meta-tags and the Learning Registry indexing (both aligned with the Common Core State Standards) this bucket will point to web-based resources.

So how will this work? First student data is shared with vendors. Then the vendors will align their products to Common Core. Internet searches on standards and instructional materials will point to Common Core-aligned resources developed by these vendors. Soon, when you search for education on the Internet, the bulk of the search will be Common Core related.

Clearly this narrows the education enterprise and raises issues of anti-trust and control of the Internet. And what will be the impact on the privacy of students' records? inBloom has stated that it "cannot guarantee the security of the information stored ... or that the information will not be intercepted when it is being transmitted." The question is: Should we compromise and endanger student privacy to support a centralized and profit-driven education reform initiative?

Given this new landscape of an information and data free-for-all, and the proliferation of data-driven education reform initiatives like Common Core and huge databases of student information, we've arrived at a time when once a child enters a public school, their parents will never again know who knows what about their children and about their families. It is now up to individual states to find ways to grant students additional privacy protections.

Privacy expert Daniel Solove said: "Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone."