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

Education NEW YORK

When the Family Educational Rights and Privacy Act (FERPA) was enacted in 1974 student data and records existed in an almost completely non-digital environment. More than three decades later, issues of data and information privacy have become of paramount concern to the public, especially to families trying to protect their children's personal information from marketers and advertisers, identity theft, and from those who might do children harm.

But the proposed rule changes to FERPA to accommodate the statewide collection and warehousing of a range of student educational, personal, and employment data and information make clear that the time has come to reconsider whether the law has outlived its ability -- and its original purpose -- to protect student privacy. In the digital age, the line between supposedly secure school directories and the online world is rapidly disappearing. Computer security breaches are rampant, exposing private and proprietary information in online databases. Hackers aggressively target large databases every day. The recent breach of the Sony Playstation database exposing the personal information of 100 million users is but one example of hackers' capabilities. Yet, the proposed FERPA rule changes would authorize more individuals, organizations, and government agencies to have access to students' personal and education information, ensuring that privacy breaches will be rampant and, in the event of a statewide database breach, potentially catastrophic.

Given this environment, proposed rules changes to FERPA should have the overriding goal to strengthen protections of student privacy and provide serious consequences for breaches of student privacy. Unfortunately the proposed changes do not meet these challenges and, in fact, would create more opportunities for student privacy to be compromised. While proposed changes take some positive steps toward giving schools and parents more control over how and when students' personally identifiable information (PII) will be released, and to whom, the changes do not go far enough to address the myriad and complex challenges of the digital age. Schools are stewards of students' personally identifiable information and as such must adhere to the highest standards of practice in protecting privacy and confidentiality. Those high standards are not met by the proposed changes, nor by the statute itself.

The proposed changes to FERPA do not adequately address the capacity of marketers and other commercial enterprises to capture, use, and re-sell student information. Even with privacy controls in place, it is also far too easy for individuals to get a hold of student information and use it for illegal purposes, including identity theft, child abduction in custody battles, and domestic violence. Few parents are aware, for example, that anyone can request -- and receive -- a student directory from a school. Data and information breaches occur every day in Pre-K-20 schools across the country, so that protecting student privacy has become a matter of plugging holes in a dyke rather than advancing a comprehensive policy that makes student privacy protection the priority.

In large part, the proposed changes are driven by the development and expansion of Statewide Longitudinal Data Systems (SLDS) and by efforts to use the SLDSs to audit and evaluate state and local education programs under the America Competes Act and with federal support from the American Recovery and Reinvestment Act (ARRA). It is important to note that ARRA was an economic stimulus and job-creation legislation, not an education mandate. Through ARRA funding for Race to the Top, the Administration is advancing statewide student Pre-K/early learning through workforce databases that would collect information from schools and share with an extensive list of agencies and organizations that may touch the life of a student: state departments of labor, child welfare, social services, juvenile justice, criminal justice agencies, employers, etc.

The federal Government Accounting Office (GAO) has studied this issue in regard to the linking of PII to employment information and exposing information such as social security numbers. In its September 2010 report, the GAO called on the DoE to clarify FERPA in regard to the collection and sharing of employment information.[1] While the proposed rule changes to allow the non-consensual disclosure of students' PII to the vaguely defined "authorized representative" may be in response to the GAO report, the "clarification" increases the potential for privacy breaches.

As noted in the comment of Paul Gammill, former head US Department of Education's Family Policy Compliance Office, filed May 17, 2011:

[1] "Postsecondary Education: Many States Collect Graduates' Employment Information, but Clearer Guidance on Student Privacy Requirements is Needed," GAO, September 2010.

Sections (b)(1)(C), (b)(3) and (b)(5) of FERPA (20 U.S.C. 1232g (b)(1)(C), (b)(3) and (b)(5)) of the statute clearly identify and permit only four entities to disclose PII without consent. These four were established by statute and have been unchanged for many years thus these need to be expanded by statute alone. While the NPRM explains the desire to greatly expand the list of such "authorized representatives" such a clearly defined and established statute cannot be expanded by a regulatory change. Such an expansive regulatory change to established statutory law exceeds the legal authority of the Department.

The rule changes to make student information more available to SLDS, researchers, and other government agencies likely will also have the effect of creating a new market for data-poachers that will be difficult to control. Few schools or statewide databases are technologically equipped to defend themselves against significant data breaches, and they would be more vulnerable under the proposed rule changes. The sophisticated electronic systems used to identify and breach the privacy of individuals should not have access to the PII of vulnerable students.

One 50-state study of longitudinal databases found they contained excessive amounts of detailed student information in non-anonymous student records, with a lack of effective privacy protections.[2] The study found that states were collecting PII, demographics, disciplinary records, academic records, health information as well as information about families. For example, the study found at least 32 percent of the states "warehouse" students' social security numbers, 22 percent have records of students' pregnancies, and an astounding 46 percent of the states include mental health, illness, and criminal justice records in educational records. More than 80 percent of states do not appear to have data-retention policies, increasing the chance that they may hold student information indefinitely. The lack of data-retention policies may have the effect, for example, of preserving a student's juvenile criminal justice record in his or her education file even when those records have been sealed or expunged.

In addition, this study found that several states outsourced the data-warehousing function without any protections for privacy in vendor contracts.

[2] Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems, Joel R. Reidenberg and Jamela Debelak, Fordham Center on Law and Information Policy. 2009.

As states move forward with SLDS, more stringent privacy protections need to be in place. Although the Department maintains that the Fair Information Practice Principles (FIPP) underlie its privacy initiatives, the proposed rule changes will compromise those principles in some significant ways. The principles of FIPP, as outlined by the Federal Trade Commission, provide for notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.

First, few parents are aware of FERPA and how it is designed to protect their child's privacy in pre-K through 20 schools -- and now to the workforce. In fact, FERPA is usually associated with higher education and the privacy of college and university education records. Schools have been found to have varying degrees of conformance with the basic FERPA notice requirements to parents and guardians under FERPA. The opt-out system under which parents must file a form with the school to keep their children's PII from being shared is inherently weak and tantamount to de facto consent. Opt-out is a regular practice of marketers and advertisers who know that few consumers will take affirmative action to remove their name and information from a list. Students and their families deserve a more proactive system of consent than opt-out.

FERPA has historically lacked effective enforcement measures and has provided little in regard to redressing student privacy breaches. The proposed rule change to sanction the “redisclosure” of PII from education records does not consider the myriad ways the security of education records can be breached or the ways student information can be mishandled or how inaccurate information can harm a student. In addition, since under the proposed change the sanction would only apply to “an authorized representative of a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3),” how would privacy breaches involving other individuals or entities not included in that definition be sanctioned? There appears to be no sanctions or redress for use and disclosure of PII by those not covered under the FERPA definition. When the proposed rule changes have the potential to lead to serious breaches of student privacy, thereby compromising the safety and security of children and young people, the need is even more urgent for strict and enforceable sanctions. The lack of meaningful sanctions and enforcement of student privacy violations under FERPA seriously weakens its authority and again calls into questions its continued usefulness in the digital age.

The proposed rule changes raise the larger question of how the privacy of children will be protected going forward. The divide between how we protect the privacy of "children" vs. "students" under the law is too wide, leaving the privacy, safety, and security of children at risk.

Currently, the online collection of personal information from children under age 13 is protected under the Federal Trade Commission's Children's Online Privacy Protection Act (COPPA). COPPA provides a useful framework for protecting student privacy. COPPA outlines requirements of a website operator's privacy policy, when, and how to seek verifiable consent from parents, privacy protections for children, and restrictions on marketing to children. Yet, an individual or entity could obtain a student directory with email addresses and telephone numbers and contact students directly without fear of legal action. Students need more robust privacy protections than this for their personal information maintained by schools they attend. However, students are not mentioned in the current privacy and consumer protection bills. While "children" are discussed in COPPA, Congress generally remains silent on protecting the sensitive and personally identifiable information of students. Clearly, it is time for Congress to consider children's privacy in its totality and without regard to federal policy goals or funding opportunities.

Absent strong federal laws to protect student privacy, states may take action to tighten restrictions on what FERPA would allow. New York is one state seeking to advance stronger privacy protections than those available under FERPA. New York State Sen. Suzi Oppenheimer (D-Mamaroneck), a longtime member of the Senate education committee, has sponsored a bill that restricts the use of any directory information for profit-making. The bill also categorizes directory information, requiring affirmative consent for the release of sensitive information. The bill is in the process of being amended. UPDATE: SPONSOR: Oppenheimer S.2357 Jun 17, 2011: PASSED SENATE: 62-0. (http://m.nysenate.gov/legislation/bill/S2357B-2011) ;
June 17, 2011: A8474-2011 Introduced in Assembly by Assemblymember Rosenthal, SPONSOR: Rosenthal; CO-SPONSOR: Nolan. (http://m.nysenate.gov/legislation/bill/A8474-2011) ; June 17, 2011: Referred to Education Committee.

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."[3] As states collect a trove of information and data for the SLDS, the security of students' information will be put at greater risk and their privacy will be further eroded. With students' PII increasingly digitized and shared electronically, the need for enhanced privacy protection is greater than ever. Students deserve the highest level of protection possible. Under FERPA, a law enacted to specifically protect the privacy of students' educational records, protections should meet the highest standards available. The proposed rule changes to FERPA fail to meet these standards nor do they adequately address the gathering threats to student privacy in the 21st century.

May 23, 2011

[3] "Why Privacy Matters Even if You Have 'Nothing to Hide'," by Daniel J. Solove, The Chronicle Review, May 15, 2011.