PRIVACYTRACKER
An IAPP members-only blog on privacy legislation

Protecting Student Data at the State Level: A Proposal for CPOs in DoEs

By Sheila Kaplan

Last year, Fairfax County, Virginia, Public Schools discovered that the names, ID numbers, grades and other information for students in grades nine through 11 had been posted online. The school district was forced to go to federal court to get the website posting the information to remove it from the site. In the meantime, the private information of more than 2,000 students was available online for several days for anyone to see and misuse.

Unfortunately, this large-scale breach of student privacy is not a rare occurrence. Breaches happen regularly, and we can expect more as educational institutions share student data with greater frequency.

Incidents like the one in Fairfax demand that we provide greater protections for students' education records. I've read about hundreds of incidents of data breaches during the past seven years of tracking student privacy practices and policies across the country.

Since 2011, my focus has been primarily on informing parents and students of their right to opt out of allowing their school to make their directory information available to third parties.

Even though my Opt-Out campaign gained traction and attention, I became frustrated with the inadequacy of the Family Educational Rights and Privacy Act (FERPA) to protect the privacy and security of student records. Recent state-level bills also have missed the mark, failing to keep up with the complex challenges presented by statewide collection, use and sharing of student and school data by government agencies and private companies.

What to do?
In order to address these issues comprehensively, each state needs a Chief Privacy Officer in its Department of Education (DoE). The broad goal of a CPO is to promote the implementation of fair information practices for privacy and security of personally identifiable information (PII). Working with privacy experts, I drafted the model bill Chief Privacy Officer for Education Act that can easily be adapted to meet states' needs.

The problem with FERPA
FERPA was enacted in 1974 to protect the privacy of school records and directory information. Directory information can include a student's name, address, phone number, date and place of birth and e-mail address, among other PII.

FERPA's data restrictions were generally good until recently when the federal DoE revised the rules to remove traditional limitations prohibiting educational institutions and agencies from disclosing students' PII without first obtaining student or parental consent.

That change opened the door for more sharing of student data through data-driven education initiatives like Common Core State Standards—and as cloud computing becomes more ubiquitous and specially designed tablets replace books and drive curriculum. Whether you support or oppose these initiatives on their own merits, there is no question that they increase the trafficking of student data.

Why tackle this at the state level?
Federal rules allow state privacy laws to provide additional protections for student information, so now that the federal DoE has abandoned its role as a protector of student privacy, it is up to the states to step in to protect students and families.

The risks
Records maintained by schools about students, teachers, employees, alumni, contributors and school board members contain a range of PII, including health and financial information as well as educational data. The use and disclosure of that information affects the rights, interests, future and, potentially, the safety of those individuals and their families.

The Federal Trade Commission has raised the alarm on student privacy, offering a Consumer Alert to parents warning of the risk of children's identity theft and urging parents to safeguard their children's school records and directory information.

But the risks are not just that student data will be disclosed improperly. Another concern is that new databases originally intended for education will become lifetime repositories of each individual's activities from cradle to grave.

The fear is that student databases will eventually expand their functions in predictable and unpredictable ways, in much the same way that the function of Social Security numbers and credit reports have grown over the years. Will a record of a temper tantrum in second grade keep someone from boarding an airplane 30 years later?

"Schools are often not handling privacy issues very well," writes privacy expert Daniel Solove, who notes that parents have little awareness of how education technology is tracking their children.

Why the CPO proposal makes sense
Given this urgent need for privacy protections, a statewide CPO for education would be the right office to act as the primary gatekeeper and expert on privacy and security matters related to students and their families as well as education institutions and agencies.

Joel Reidenberg, an expert on information technology law and policy, has made a strong case for the state education CPO position, telling the U.S. House of Representatives Committee on Education and Labor: "A Chief Privacy Officer in the state departments of education would, like the CPOs in the federal Department of Homeland Security and Department of Justice, provide transparency to the public and oversight for compliance with privacy requirements."

Under the proposed model bill, the CPO would advise students, parents and other individuals about options and actions that they can take to protect the privacy and security of PII; make recommendations on privacy and security to the governor, state

legislatures and agencies, schools, parents and students; and conduct oversight of privacy and security activities of organizations handling and storing student data.

Students deserve a true advocate for their rights in a data-driven environment that often places profit and corporate interests above the privacy rights of children and their families. Those who bear responsibility for student records need a reliable resource to help them manage their obligations. Those who make decisions about proper use of student records also need more policy direction.

A state CPO for education would serve the public interest by providing needed expertise to school data managers and users by advising policy makers and by helping students, families, teachers and others to protect their privacy rights and interests.

Sheila Kaplan is a longtime independent education and information policy researcher and publisher and an advocate for students' rights. She is the founder of Education New York Online, a comprehensive source of education and information policy and research and children's privacy rights matters. Sheila is a member of the advisory board of the Electronic Privacy Information Center (EPIC). She is executive director of the William and Elaine Kaplan Family Private Foundations.

This article was originally published in the IAPP's *Privacy Tracker* blog.