Testimony
By Sheila Kaplan
Founder, Education New York

Assembly Standing Committee on Education
Public Hearing
Hamilton Hearing Room B
Legislative Office Building, 2nd Floor
Albany, New York
November 20, 2013

Thank you Assemblywoman Nolan and Committee Members for this opportunity to testify today.

I am Sheila Kaplan, founder of Education New York and a longtime independent education and information policy researcher and publisher as well as an advocate for students' privacy rights. I am also a member of the advisory board of the Electronic Privacy Information Center, a leading privacy and civil liberties advocacy organization based in Washington, D.C.

I want to talk about the current and emerging threats to student privacy in New York, including the disclosure of personally identifiable student information by the State, school districts, and schools.

I also will offer a policy proposal that addresses the urgent need for the State to take action to protect students' rights by providing oversight of the security and privacy of their data and information.

It is important to note that the issues being considered by the Assembly today are not strictly education policy matters, but rather involve important questions in information policy that all institutions, organizations, and government agencies deal with today. Regardless of the specifics of federal and state education policies under consideration, the age of data-driven policies and practices is here to stay – and will grow even more complex in the years to come.

My work has focused on helping to ensure that Fair Information Practice Principles – guidelines that are widely accepted by entities in the U.S., Canada, and Europe that collect and use personal information – are applied to students and their personally identifiable information and data. For example, I have worked over the last seven years to raise awareness of the limits of the Family Educational Rights and Privacy Act (FERPA) to protect the privacy and security of student records, as well as the need for state action to protect students. **[See Exhibit 1, Student Privacy Protection Act; attached.]**

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 personally identifiable information, or PII.

However, the privacy and security of school records and directory information remains at risk despite the protections of FERPA. In fact, the Federal Trade Commission has raised the alarm on student privacy, warning

of the risk of children's identity theft and urging parents to safeguard their children's school records and directory information.

To further inform parents and students of their rights under FERPA, in 2011 I launched a national Opt-Out Campaign. The campaign raises awareness of the right to opt out of allowing schools to make students' directory information available to third parties.

However, overall, FERPA has fallen short in protecting student privacy and safety. Further compromising the privacy of students' records, the federal Department of Education revised the FERPA rules two years ago to remove traditional limitations prohibiting educational institutions and agencies from disclosing students' PII without first obtaining student or parental consent.

The risks are not just that student data will be disclosed improperly.

There is a worry 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 has grown over the years.

Will a record of a temper tantrum in second grade keep someone from boarding an airplane 30 years later? And consider the ubiquity of cameras, which along with algorithms and facial recognition software can identify students from photos posted on social media and connect those images with their PII.

The challenges to student privacy and security of student data extend beyond the classroom and school building. Today, schools and curriculum may

require students to complete assignments at home using tablets that include cameras and microphones. The audio and visual data is transmitted via Wi-Fi or cellular connection provided by the company that produced the tablet.

One need only look at a case in Pennsylvania to see the dangers inherent in this use of technology. According to the American Civil Liberties Union of Pennsylvania, which represented a student in the case, **"**The Lower Merion School District has admitted publicly that it activated a tracking system in student laptops at least 42 times during the 2009-2010 school year alone, each time capturing dozens or hundreds of photographs of the laptops' surroundings, as well as collecting the information on the computer screen."

Students are immersed in the world of social media – a world that often intersects with their lives in school, with sometimes tragic results in the case of recent bullying episodes. Therefore, the protection of the privacy rights of the individual, especially children, must be addressed as one of the most pressing issues of our time.

Schools need guidance on developing policies to protect student privacy when social media is used for education purposes – such as a Facebook page created by a teacher for a class. Especially given the focus on online bullying, social media guidelines to ensure student privacy are of utmost concern.

Cloud computing also has become more ubiquitous in education and specially designed tablets are replacing books and driving curriculum. The increasing use of the cloud storage creates yet another way a student education record is maintained and handled, necessitating additional privacy

and security protections. According to privacy expert Daniel Solove: "Schools are often not handling privacy issues very well." He notes that parents have little awareness of how education technology is tracking their children **[See Exhibit 2, K12 Student Privacy and Cloud Computing Act; attached.]**

While cloud computing is allowed under FERPA, the law does not provide explicit rules on handling student data in the cloud, leaving schools and education institutions to develop their own "common sense" guidelines. **[See Exhibit 3, Daniel Solove, Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education; attached.]**

Now that the federal Department of Education has abandoned its role as a protector of student privacy, it is up to the states to step in to protect students and families. Federal rules *do* allow state privacy laws to provide additional protections for student information, which opens the door to state action. The most important action the State can take at this time to protect student privacy is to create the position of Chief Privacy Officer in its Department of Education.

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 broad goal of a CPO is to promote the implementation of fair information practices for privacy and security of personally identifiable information (PII). **[See Exhibit 4, Chief Privacy Officer for Education Act; attached.]**

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.

Joel Reidenberg, a nationally recognized expert on information technology law and policy, also 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." **[See Exhibit 5, Statement of Joel R. Reidenberg; attached.]**

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.

Those who bear responsibility for student records need a reliable and expert 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.

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. A state CPO for education would serve the public interest to protect the privacy rights of students and their families – and help prevent data breaches that put the future and safety of large numbers of students at risk.

Student Privacy Bills

There are two Assembly student privacy bills under consideration at this hearing. While this is the right time to take action to protect student privacy, it is important that they do so in a way that makes a meaningful difference. The following comments are offered with that goal in mind.

A.7872 – Relates to the release of personally identifiable student information

This bill is well-intentioned, but it is troubling in a variety of ways. First, the bill's reliance on opt-out may be misplaced. We know from both online and offline experience that people usually accept the default choice. If the default allows a disclosure unless you opt-out, 95% of people will do nothing and not opt-out. If the default rejects a disclosure unless you opt-in, 95% of people will do nothing and not opt-in. Providing an opt-out selection provides the appearance of choice, but the reality is that someone's thumb is very heavily on the scale. An opt-out will not really change anything.

My own legislative proposal, the **Student Privacy Protection Act**, strikes a better balance for directory information about students. It combines 1) affirmative notice; 2) opt-outs only for disclosures to school newspapers, yearbooks, honor rolls, and the like; 3) opt-in notice for PTAs and other non-

profits; and 4) a flat ban on disclosures for commercial activities even with affirmative consent. I suggest that this is a more nuanced approach to directory information that fairly balances the many competing concerns and the realities of choice. Parents can already opt- out of directory information disclosures, but few do because they don't understand the issue. We need to do better than to offer parents and student an opt-out that won't make a difference.

Second, A.7872 does not provide an opt-out for longitudinal databases maintained by third parties out of state. Many people are concerned that the maintenance of longitudinal databases about students will adversely affect their children in ways that are both unfair and out of their control. The bill ignores these concerns entirely.

Third, the bill allows parents/students to opt-out of some disclosures that could undermine legitimate activities. If a parent/student signs a blanket opt-out without thinking about or understanding the details, then activities such as student financial aid, juvenile justice, alcohol/substance abuse, sex offender registration, disciplinary proceedings, and even school accreditation could be negatively affected. What would happen if an alleged perpetrator opted out of disciplinary proceeding disclosures? That could fatally undermine the proceeding. Why would anyone allow that to happen?

The scope of the opt-outs allowed by A.7872 needs to be rethought. The list of possible non-consensual disclosures (found in the FERPA rule at 34 CFR § 99.31) needs to be reviewed with greater care.

A.6059 – Prohibits the release of personally identifiable student information where parental consent if not provided

A.6059 is an ambitious bill that includes several privacy-protecting features. A major part of the bill controls the conditions under which student information can be shared with third parties. These conditions extend beyond the protections in FERPA and are much more carefully adapted to problems that schools and student face today. I offer comments on some features of the bill and suggest some technical changes for consideration. However, many of the conditions, including those pertaining to use and disclosure limits, security, and security breaches, are needed.

Section 2(d) prohibits non-consensual disclosures for commercial purposes but allows disclosures with parent/student consent. A consent for this purpose must be signed dated on the day it was signed, not have been signed more than six months prior to the disclosure, must identify the recipient and the purpose of the disclosure, and must state that the information will only be used for that purpose and will not be used or disclosed for any other purpose. I suggest an improvement to the consent in the list of technical changes below.

Limits on disclosures for commercial purposes are welcome. For directory information, at least, I suggest again that a different approach may be appropriate. My legislative proposal, the **Student Privacy Protection Act**, bans most commercial disclosures even with consent. A parent or student

that wants to share personal information with a commercial entity can always do so on their own. There is no reason for a school to play any role as an agent of commercial database companies or others. Schools should not have any incentive to do so and should never be allowed to profit from the commercial sale of student data. Allowing schools to sell student data under any conditions creates a conflict between the school's financial interests and its role as protector of students.

Many of the other provisions of the bill would have positive effects on the privacy of student information. Implementing the bill will not be simple. I suggest that schools, student, parents, and the Department of Education would benefit if A.6059 included a **Chief Privacy Officer for Education**. I have a complete legislative proposal for a CPO who could provide guidance and oversight of the privacy features of A.6059. Enforcement by the Attorney General as provided in the bill is fine, but schools will need help to do the right thing in the first place.

Technical/minor amendments to A.6059

1. Section 2(b) regulates outsourcing for institutional services or functions without parental/student consent. However, it is not clear why parental or student consent would be appropriate for outsourcing in the first place or why it would ever be sought by any school. The consent language on page 2, lines 10-11 should be dropped.

2. The conditions in Section 2(b) that apply to outsourcing could be improved in several ways.

a. Condition 5 allows a contractor to disclose with consent. It is not clear why this should be allowed. A consent casually signed by a parent or student for another purpose could allow a contractor to disclose student records. That seems inappropriate. A consensual disclosure should be arranged through the school and not directly with the school's contractor.

Perhaps the possibility of disclosure with consent should be removed or disclosures should be prohibited without the prior written consent of the department, district board of education, or institution that provided the information. The organization that provided the information to the contractor should make decisions about subsequent disclosures, perhaps only with parent/student consent. Alternatively, if parental/student consent can be justified, then only a consent that refers to this provision of law should be acceptable. That would prevent consensual disclosures under general "any or all records" consent forms signed for other purposes.

b. Condition 8 requires that a contactor have sufficient administrative and technical procedures to monitor continuously the security of personally identifiable information in its custody. This would be improved if the words use, disclosure, and were added before security.

c. Condition 9 mandates that a contractor conducts a security audit annually. It would be better if the provision said contracts annually for an independent security audit by a qualified auditor. If a security audit can be conducted by the person being audited, the value of the audit will be minimal.

d. Condition 11 mandates that a contractor report all suspected security

breaches to the department, district boards of education, or institution that provided education records as soon as possible but not later than forty-eight hours after a suspected breach was known or would have been known by exercising reasonable diligence. The last clause (or would have been known by exercising reasonable diligence) presents a logical impossibility. If a person should have known of a breach by reasonably diligence but did not know in fact, it is impossible for that person to have reported the breach after it "would have been known." The last clause should be dropped.

e. Condition 12 has the same language (or would have been known by exercising reasonable diligence) as condition 11. That language should be dropped for the same reason.

3. The last sentence of Section 2(d) sets conditions for a signed consent. The last sentence of the section would be improved with the addition of the underlined requirement:

Any consent from an eligible student or parent must be signed by the student or parent, be dated on the day it was signed, not have been signed more than six months prior to the disclosure, must identify the recipient and the purpose of the disclosure, must reference this section of law, and must state that the information will only be used for that purpose and will not be used or disclosed for any other purpose.

The purpose is to require that consent specifically mention this particular section. This additional requirement will prevent a general "any or all records" consent signed casually for another purpose to be used to obtain

NY educational records.

4. Section 3(b) requires public and legislative reporting about student data repositories. Paragraph (1) addresses name and location. Location is not meaningful today given the Internet and the cloud. A change will make the disclosure more useful and will provide more information about cloud storage. Strike the existing language and insert in lieu:

(1) The name of each person or entity that maintains, stores, or has physical or electronic possession of the data repository, the address of that person or entity, and, where a third party provides electronic storage of the data repository for the person who placed the data in the repository, any contractual or other authority claimed by the third party to access, use, or disclose data in the repository.

5. Section 3(c) limits data matching with PII from other federal or state agencies, with suitable exceptions. Importantly, it does not cover data matching using records from sources that are not agencies. Thus, matching using commercial records would be allowed without limit, but matching using state records would be subject to the exceptions. A simple amendment will suitably broaden the prohibition on data matching.

(c) the department, district boards of education, and institutions may not append education records with personally identifiable information obtained from other sources federal or state agencies through data matches without the written consent of eligible students or parents unless such data matches are: (1) explicitly mandated in federal or state statute; or (2) administratively

required for the proper performance of their duties under the law and are relevant to and necessary for delivery of services.

The amendment would regulate all data matching if the data were obtained from a source other than the department, district boards of education, and institutions. Allowing for use of commercial sources under the administratively required standard is probably appropriate. For example, a school might use a commercial service to update mailing addresses. This type of match would be allowed under the amendment.

Model State Law

Student Privacy Protection Act

Section 1. Title

This Act shall be known and cited as the "Student Privacy Protection Act." This Act shall be liberally and remedially construed to effectuate its purpose. The purpose of the Act is to protect the privacy of students by establishing standards for the disclosure of directory information about students by schools.

Section 2. Definitions

(a) "School" means any [public school, any non-public school of secondary education, and any school of higher education].

(b) "Student", "directory information", "eligible student", and "personally identifiable information" have the same meaning as in 34 Code of Federal Regulations Part 99.

(c) "Personally identifiable student information" means personally identifiable information and directory information.

(d) "Disclosable directory information" means with respect to a student, the student's name; photograph; age; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended.

Section 3. Limits on Disclosure of Student Information

(a) A school shall disclose personally identifiable student information about a student to the parent of the student or to the eligible student in accordance with applicable law.

(b) A school may disclose directory information about a student as provided in 34 Code of Federal Regulations Section 99.37 only:

> (1) after giving the parent of the student or the eligible student at the school notice and an opportunity to opt-out of the disclosure in accordance with Section 4;
>
> (2) if the disclosure does not include any personally identifiable student information other than disclosable directory information; and
>
> (3) if the disclosure is to a school newspaper; local newspaper; school club or organization; school yearbook; honor roll or other recognition list; graduation program; sports related publication which provides specific information about

particular students for the purposes of a specific sports activity or function; or parent and teacher organization.

(c) A school may disclose personally identifiable student information with the affirmative consent of the parent of the student or the eligible student in accordance with the procedure described in section 4(b)(3) of this Act if the disclosure is to a non-profit organization:

(1) that states in writing that it seeks the information for a specific identified purpose determined by the school to be in the educational interest of the student;

(2) that states in writing that it will use the information only for the specific identified purpose and will return or destroy the information when the purpose has been fulfilled, but not later than one year after receipt;

(3) that states in writing that it has not used or disclosed personally identifiable student information from any school in a manner inconsistent with the terms of disclosure within the past five years; and

(4) if the school has no reason to believe that the recipient used or disclosed personally identifiable student information from any school in a manner inconsistent with the terms of the disclosure within the past five years.

(d) Unless otherwise expressly allowed by law, a school may not disclose personally identifiable student information about a student, even with the affirmative consent of the parent of the student or the eligible student, for any commercial, for-profit activity, including but not limited to use for:

(1) marketing products or services;

(2) selling or renting personally identifiable student information for use in marketing products or services;

(3) creating, correcting, or updating an individual or household profile;

(4) compilation of a list of students;

(5) or any other purpose considered by the school as likely to be a commercial, for-profit activity.

(e) In making an allowable disclosure under section 2 of this Act, a school may only disclose the minimum amount of information necessary to accomplish the purpose of the disclosure.

Section 4. Notice

(a) Within the first week of each school year, each school shall issue a public notice, include in a student or parent handbook, and provide to each student in a form that the student can retain or

give to a parent, information describing the school's disclosure procedures for personally identifiable student information.

(b) The information required under subsection (a) shall include:

(1) a description of any personally identifiable student information that the school expects to disclose during the school year;

(2) the procedure that a parent of a student or an eligible student can follow to prohibit the school from disseminating disclosable directory information under section 3 of this Act; and

(3) the procedure that a parent of a student or an eligible student can follow to authorize the school to disseminate personally identifiable student information under section 3 of this Act.

(c) If the school does not receive an objection from the parent of a student or the eligible student within thirty days of the dissemination of the information required to be provided under subsection (a), the school may disseminate disclosable directory information relating to the student pursuant to section 3 of this Act..

Section 5. Effective Date

This Act shall take effect on July 1 following the date of enactment. If there is less than six months between the date of enactment and July 1, the Act shall take effect on July 1 in the year following the date of enactment.

Bill S5355-2013

Enacts the "K12 student privacy and cloud computing act"

Enacts the "K12 student privacy and cloud computing act" to prohibit service providers who offer cloud computing services to primary and secondary educational services from processing student date for commercial purposes.

Details

- Same as: A7243-2013
- Versions S5355-2013
- Sponsor:MAZIARZ
- Multi-sponsor(s): None
- Co-sponsor(s): PARKER, SAMPSON
- Committee: EDUCATION
- Law Section: Education Law
- Law: Add §755, Ed L

Memo

BILL NUMBER:S5355

TITLE OF BILL: An act to amend the education law, in relation to enacting the "K12 student privacy and cloud computing act" to prohibit service providers who offer cloud computing services to primary and secondary educational institutions from processing student data for commercial purposes

PURPOSE: OF THE BILL: To ensure that when an educational institution (primary and secondary) engages a cloud computing service provider and such provider has access to student data, such data may only be used to benefit the educational institution and may not be used for the provider's own commercial purposes, including profiling for the purposes of marketing and advertising.

SUMMARY OF SPECIFIC PROVISIONS:

Section 1 refers to the measure as the "K-12 Student Privacy and Cloud Computing Act."

Section 2 sets forth legislative intent.

Section 3 establishes a new section in the Education Law to address the issue of cloud computing and student privacy.

Subdivision 1 establishes definitions.

Subdivision 2 prohibits any person who provides a cloud computing service to an educational institution from processing student data for any commercial purposes, including but not limited to advertising, marketing products or services, creating or correcting an individual or household profile and sale-of the data. An exception is made for the processing of data necessary to provide the service to the educational institution or maintain the integrity of the system.

Subdivision 3 provides that, upon entering into an agreement with an educational institution, a cloud computing service must certify in writing to the institution that shall comply with this act.

Section 4 is the effective date.

JUSTIFICATION: As more and more schools have adopted advanced information technology platforms as essential components of their educational program, policy-makers have demonstrated concern about the implications of student privacy in the digital age. To that end, Congress has enacted the "Family Education Rights Privacy Act" (FERPA) and the "Children's Online Privacy Protection Act" (COPPA), to address some of these concerns.

Under FERPA, schools are required to notify parents at the beginning of the school year of the right to "opt out" of school disclosure of a student's personally identifiable information. While the benefits and flaws of FERPA are much debated - it simply does not address the challenges presented by a cloud-computing service provider (CSP) accessing and processing student correspondence, school work product, photographs, social networking and other information.

COPPA, on the other hand, regulates the online collection, use and disclosure of personal information from children under 13 by operators of websites and online services that are directed to children including, in certain cases, CSPs. COPPA generally applies to websites and online services operated for commercial purposes, but may also apply to schools that offer students access on online services such as email and that are operated for commercial purposes. COPPA does not apply to a CSP's online collection of information from students under the age of 13 as long as the collection of information is for the sole use and benefit of the school. If, however, the CSP uses the collected information for commercial purposes, then COPPA applies.

If COPPA does apply to a CSP who uses the student's data for commercial purposes - the behavior is not barred, but rather the following steps must be taken by the CSP:

1. Notice must be sent to the parent and verifiable consent must be obtained;

2. The CSP must post a clear privacy notice on its website or online service that explains what personal information is collected from children and how it is used;

3. Limits must be placed on the collection of personal information that is necessary to participate in the online activity;

4. Parents are to be provided with an opportunity to review and delete their children's personal information;

5. The confidentiality, integrity and security of the children's personal information must be protected.

Finally, COPPA also requires that an educational institution obtain permission from a parent before using the online service.

While well-intended, in practicality, COPPA falls short of adequately insulating students (and parents) from wide-spread data collection and profiling. In fact, under COPPA, schools are being asked to monitor activities that they may be ill-equipped to oversee; while the few parents who are actually aware of what is at stake, have to choose between their child's privacy and the child's access to the same cloud services that the other students are using. Moreover, COPPA only applies to students

under the age of 13.

A recent study by Brunswick Insight* published this year revealed interesting results. In the study more than 1000 American parents with children in grades K-12 were surveyed. Despite the privacy requirements of FERPA and COPPA, there is a significant "awareness problem". As parents were informed of the collection and use of data related to their children:

* 75% of parents disapproved of CSPs tracking online behavior to build profiles;

* 75% of parents objected to CSPs using data collected from in-school email and Internet usage in order to target students with Internet advertising;

* 76% disapproved of CSP's using additional service offerings, such as video sharing or social networking, to get around privacy agreements and collect children's personal information and track their online behavior; and

* After receiving more information about online tracking and data mining, an astounding 64% indicated that they would like to take action against those practices.

Beyond awareness, there is an additional challenge. A recent study by Professor Daniel Solove** concluded that K-12 educational institutions did not have the expertise or personnel to manage privacy issues. For example, his research failed to reveal a single Chief Privacy Officer at any K-12 educational institution anywhere. Yet, in light of what we know about protecting personal privacy, every school should be able to tell you what steps they are taking to protect their children's privacy; every school should be able to tell you about online tracking by any of their cloud or online vendors; every school should be doing online privacy audits; every school should conduct data inventory or have data stewards. Unfortunately, this is not happening.

Unlike FERPA and COPPA, this legislation acknowledges the dual realities that (1) parents are generally uninformed about the data that is being collected on their children and how it is being used, but, once informed, reject that practice; and (2) our schools are not equipped to manage the privacy concerns presented by the sophisticated methods behind data mining and commercial behavioral advertising. As a result, any cloud-computing service provider doing business with educational institutions in New York should be restricted from data mining for commercial purposes and they must certify, in writing, to the same.

PRIOR LEGISLATIVE HISTORY: New Bill

FISCAL IMPLICATIONS: None to the State; but will relieve school districts of some financial obligations associated with complying with certain provisions of FERPA and COPPA.

EFFECTIVE DATE: The first day of November next after which it has become law, provided that the commissioner of education and the board of regents are authorized to promulgate such rules and regulations as may be necessary for the timely implementation of such act on or before such effective date.

*Brunswick Insight, January 2013 (media/43502/brunswick_edu_data_privacy_report jan_2013.pdf)

**Daniel J. Solove is the John Marshall Harlan Research Professor of Law at George Washington University Law School and the founder of TeachPrivacy

(http://teachprivacy.com) and Senior Policy Advisor at Hogan Lovells. Permalink(/2013/1/8/parental-attitudes-about-student-privacy-online).

Text

STATE OF NEW YORK

5355

2013-2014 Regular Sessions

IN SENATE

May 16, 2013

Introduced by Sen. MAZIARZ -- read twice and ordered printed, and when printed to be committed to the Committee on Education

AN ACT to amend the education law, in relation to enacting the "K12 student privacy and cloud computing act" to prohibit service providers who offer cloud computing services to primary and secondary educational institutions from processing student data for commercial purposes

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Short title. This act shall be known and may be cited as the "K12 student privacy and cloud computing act".

S 2. Legislative findings. The legislature hereby finds and declares:

1. Cloud computing services enable convenient, on-demand network access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction;

2. Cloud computing services offer tremendous potential to educational institutions in terms of helping consolidate technical infrastructure, reducing energy and capital costs, increasing collaboration through "anytime-anywhere" access to applications and information, and realizing efficiencies, network resilience, and flexible deployment; and

3. Cloud computing service providers hold the potential to invade the privacy of students by tracking students' online activities for commercial purposes, such as delivering behaviorally targeted advertising or otherwise improving advertising services that the service provider may offer in connection with or separate from the services it offers to the educational institution.

In light of the foregoing, the legislature deems it necessary to ensure that when an educational institution engages a cloud computing service provider to process student data, that the service provider uses student data only for the benefit of the educational institution and does not use such data for the service provider's own commercial

purposes.

S 3. The education law is amended by adding a new section 755 to read as follows:

S 755. STUDENT PRIVACY AND CLOUD COMPUTING. 1. DEFINITIONS. FOR THE PURPOSES OF THIS SECTION, THE FOLLOWING TERMS SHALL HAVE THE FOLLOWING MEANINGS:

(A) "CLOUD COMPUTING SERVICE" SHALL MEAN A SERVICE THAT ENABLES CONVENIENT, ON-DEMAND NETWORK ACCESS TO A SHARED POOL OF CONFIGURABLE COMPUTING RESOURCES TO PROVIDE A STUDENT, TEACHER OR STAFF MEMBER ACCOUNT-BASED PRODUCTIVITY APPLICATIONS SUCH AS EMAIL, DOCUMENT STORAGE AND DOCUMENT EDITING THAT CAN BE RAPIDLY PROVISIONED AND RELEASED WITH MINIMAL MANAGEMENT EFFORT OR CLOUD COMPUTING SERVICE PROVIDER INTERACTION.

(B) "CLOUD COMPUTING SERVICE PROVIDER" SHALL MEAN AN ENTITY, OTHER THAN AN EDUCATIONAL INSTITUTION, THAT OPERATES A CLOUD COMPUTING SERVICE.

(C) "EDUCATIONAL INSTITUTION" SHALL MEAN ANY PUBLIC OR NONPUBLIC SCHOOL, CHARTER SCHOOL, SCHOOL DISTRICT OR BOARD OF COOPERATIVE EDUCATIONAL SERVICES SERVING STUDENTS IN GRADES KINDERGARTEN THROUGH TWELFTH GRADE.

(D) "PERSON" SHALL MEAN INDIVIDUAL, PARTNERSHIP, CORPORATION, ASSOCIATION, COMPANY OR ANY OTHER LEGAL ENTITY.

(E) "PROCESS" OR "PROCESSING" SHALL MEAN TO USE, ACCESS, MANIPULATE, SCAN, MODIFY, TRANSFORM, DISCLOSE, STORE, TRANSMIT, TRANSFER, RETAIN, AGGREGATE, OR DISPOSE OF STUDENT DATA.

(F) "STUDENT DATA" SHALL MEAN ANY INFORMATION OR MATERIALS IN ANY MEDIA OR FORMAT CREATED OR PROVIDED BY: (I) A STUDENT IN THE COURSE OF THE STUDENT'S USE OF THE CLOUD COMPUTING SERVICE; OR (II) AN EMPLOYEE OR AGENT OF THE EDUCATIONAL INSTITUTION THAT IS RELATED TO A STUDENT. IN EACH CASE THE TERM "STUDENT DATA" SHALL INCLUDE, BUT NOT BE LIMITED TO THE NAME, ELECTRONIC MAIL ADDRESS, POSTAL ADDRESS, PHONE NUMBER, EMAIL MESSAGE, WORD PROCESSING DOCUMENTS, UNIQUE IDENTIFIERS, METADATA, OF A STUDENT, OR ANY AGGREGATIONS OR DERIVATIVES THEREOF.

2. PROHIBITION ON THE USE OF STUDENT DATA. ANY PERSON WHO, WITH KNOWLEDGE THAT STUDENT DATA WILL BE PROCESSED, PROVIDES A CLOUD COMPUTING SERVICE TO AN EDUCATIONAL INSTITUTION, IS PROHIBITED FROM USING THAT CLOUD COMPUTING SERVICE TO PROCESS STUDENT DATA FOR ANY SECONDARY USES THAT BENEFIT THE CLOUD COMPUTING SERVICE PROVIDER OR ANY THIRD PARTY, INCLUDING, BUT NOT LIMITED TO, ONLINE BEHAVIORAL ADVERTISING, CREATING OR CORRECTING AN INDIVIDUAL OR HOUSEHOLD PROFILE PRIMARILY FOR THE CLOUD COMPUTING SERVICE PROVIDER'S OR ANY THIRD PARTY'S BENEFIT, THE SALE OF THE DATA FOR ANY COMMERCIAL PURPOSE, OR ANY OTHER SIMILAR COMMERCIAL FOR-PROFIT ACTIVITY; PROVIDED, HOWEVER, A CLOUD COMPUTING SERVICE MAY PROCESS OR MONITOR STUDENT DATA SOLELY TO PROVIDE SUCH SERVICE TO THE EDUCATIONAL INSTITUTION AND MAINTAIN THE INTEGRITY OF SUCH SERVICE.

3. CERTIFICATION OF COMPLIANCE. ANY PERSON WHO ENTERS INTO AN AGREEMENT TO PROVIDE A CLOUD COMPUTING SERVICE TO AN EDUCATIONAL INSTITUTION MUST CERTIFY IN WRITING TO THE EDUCATIONAL INSTITUTION THAT IT SHALL COMPLY WITH THE TERMS AND CONDITIONS SET FORTH IN SUBDIVISION TWO OF THIS SECTION.

S 4. This act shall take effect on the first of November next succeeding the date on which it shall have become a law, provided that the commissioner of education and the board of regents are authorized to promulgate such rules and regulations as may be necessary for the timely implementation of this act on or before such effective date.

Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education

by **Daniel Solove, TeachPrivacy**
Thursday, April 18, 2013

I had the pleasure of having the opportunity to interview Kathleen Styles about cloud computing in education. Styles is the first chief privacy officer of the U.S. Department of Education (ED). Previously, she served as the chief of the Office of Analysis and Executive Support at the U.S. Census Bureau. Without further ado, here's the interview.

There's a lot of controversy about storing student information in the cloud. What's your sense of this?

Glad you asked! There are a lot of misconceptions and misinformation on this subject. For starters, many people don't understand that storing data in the cloud simply means that a system's servers are physically located at a remote data center, instead of on school property. There are many reasons to store data in the cloud – including powering student information systems or learning applications, or because cloud services can be less expensive than storing the data locally.

A lot of the misunderstanding stems from the belief that data that are co-hosted in the cloud are also commingled. The truth is that there are many different types of cloud agreements, and that co-hosting data is not the same as commingling data (in the same way that strangers who happen to use the same email hosting service as you do can't see your personal email account.) There's also nothing inherently more or less secure about cloud storage compared to traditional data storage – it all depends on the specific approach and the contract terms.

Does FERPA permit cloud solutions?

The short answer is yes, that FERPA, the Family Educational Rights and Privacy Act, does permit the use cloud services. Now for the longer, legal explanation for how. As you know, FERPA protects "education records," or records containing information directly related to a student and maintained by an educational agency or institution. Some, but not all, of the records that schools typically want to store in the cloud will be protected by FERPA. For example, FERPA wouldn't govern a school's decision to house its human resource database in the cloud if that database only has information about employees, not students.

FERPA does permit schools and school districts to contract for secure cloud services. While the general rule under FERPA is that parents/students must consent before a school can disclose protected information to another party, FERPA does have exceptions, including one for school officials. Schools and school districts commonly use this exception when they need to disclose FERPA-protected information to allow a contractor to perform functions that the school or district would otherwise have used its own employees to perform.

Under the school official exception, the school or district must use reasonable methods to ensure that school officials (employees and contractors) access only those student records in which they have a legitimate educational interest. It's up to the school or district to set the proper balance of physical,

technological, and administrative controls to prevent unauthorized access. Additionally, when cloud services involve FERPA-protected information:

- The school or district must directly control the contractor's use and maintenance of education records;
- The contract has to be for services or functions the school or district would have otherwise used its employees to perform;
- The contractor must meet the criteria for "school officials" with "legitimate educational interests," as published by the school or district in its annual FERPA notification of rights; and
- The contractor must be subject to FERPA use and re-disclosure limitations, meaning that the contractor has to use the FERPA-protected information for the purpose for which it received it, and that the contractor may re-disclose that information if permitted under the terms of the contract (and, of course, provided that the school or district itself may re-disclose under FERPA).

What are cloud providers entitled to do with the student data once it is in the cloud?

First of all, the cloud provider must comply with both FERPA and the terms of the contract. The provider never "owns" the data, and can only act at the direction of the school or district.

Other terms depend on the agreement between the school and the district. The school or district could ask a cloud provider to re-disclose FERPA-protected information to another school official, such as an app developer, if that app developer also meets the criteria required for school officials (legitimate educational interest, etc.)

I've seen a lot of discussion about whether cloud providers can use the FERPA-protected information for their own purposes, such as improving their own products. A school or district could certainly require a cloud provider to do more than just store data. For instance, the school or district could also require the provider to develop products for the school or district to use with its students. During the course of providing those services, the cloud provider could use FERPA-protected information to improve the products the school or district was using. FERPA would permit the school or district to include provisions like this in its contract with the cloud provider.

On the other hand, FERPA would not allow a cloud provider to use protected data to create a product never intended for use by the school or district. Similarly it is not okay for a school or district to give FERPA-protected data to a cloud provider solely for the provider to use to develop a product to market to a school or district.

ED recently amended its FERPA regulations in 2011. Is this what permitted schools and districts to use cloud providers?

Not at all. Cloud hosting of student data has been occurring for many years, and ED recognized schools' longstanding practice of contracting out services in its 2008 regulation changes. Neither contracting out, nor cloud services are new, and neither were at issue in the 2011 regulation changes.

Who is responsible for the privacy and security of educational data in the cloud?

Schools and districts are responsible for the protection of their data, regardless of where they are stored. It doesn't matter whether the records are located in a locked file cabinet, in a server on the school premises, or on a server in the cloud.

How should students and parents be informed?

Schools and districts using the school official exception have to publish an annual FERPA notification of rights in a forum likely to be viewed by parents, such as a student handbook, on the school's website, or a direct letter to parents. This annual notification should clearly explain who constitutes a school official and what constitutes a legitimate educational interest. Students and parents who want more information about their FERPA rights can consult http://www2.ed.gov/policy/gen/guid/fpco/ferpa/for-parents.pdf.

Beyond the legal requirement, we believe parental involvement and transparency are key.Cloud computing is a much-misunderstood topic, and schools and districts should be clear about what student information they are collecting, how they are protecting it, and what they are doing with it. Parents, students, teachers should be given a forum to ask questions and express concerns.

What do you recommend for schools or districts that want to use cloud services?

Schools and districts not only need to understand fully how to comply with applicable laws such as FERPA, but also need to be familiar with best practices for ensuring data security. Schools and districts should strive to meet the spirit of the law and not just the letter.

We recommend they consult our cloud computing guidance, which describes not only what is necessary for legal compliance, but also explains best practices. The document is available at: http://ptac.ed.gov/sites/default/files/cloud-computing.pdf

Our Privacy Technical Assistance Center (PTAC), can also provide additional assistance on cloud issues, including informal consultation, webinars, or site visits. PTAC can be reached at PrivacyTA@ed.gov.

Model State Law
Chief Privacy Officer for Education Act
Version 2.0

Section 1. Title.

This Act shall be known and cited as the "Chief Privacy Officer for Education Act." This Act shall be liberally and remedially construed to effectuate its purpose. The purpose of the Act is to protect the privacy and security of personal information maintained by schools by creating the Office of the Chief Privacy Officer for Education to oversee, audit, consult, and report on matters that affect privacy and security of school records that contain personally identifiable information.

Section 2. Findings.

The Legislature finds:

(a) Privacy is a personal and fundamental right protected by Federal and State constitutional provisions and statutes.

(b) Records maintained by schools about students and others contain a wide range of personally identifiable information, often including health and financial information as well as information about educational activities. The use and disclosure of the information affects the rights and interests of those individuals and their families. In particular, information that schools maintain can permanently affect a student's educational, employment, and other future opportunities. Information that schools maintain about teachers, employees, alumni, contributors, school board members, and others can affect the future of those individuals.

(c) Personally identifiable information maintained by schools is at risk of improper use and sharing through poor privacy policies and practices; inadequate security; insufficient rules and guidance; and lack of training.

(d) Parents, students, and others are increasingly expressing concern and frustration about privacy, security, and sharing of personally identifiable information by schools.

(e) Cloud computing and other types of data storage and sharing under the control of third parties, especially those in other jurisdictions, can exacerbate existing risks as well as raise new risks. Among these risks are that cloud computing providers may claim ownership rights over personally identifiable information that schools store in the cloud; that third parties will use or disclose personally identifiable information about students improperly or without the knowledge or consent of schools, students, and parents; that personally identifiable data is at greater risk for security breaches, and that data storage and sharing with inadequate attention to the allocation of rights and responsibilities of all parties will harm students, parents, and others, and will raise costs and legal risks of schools.

(f) Lack of adequate privacy and security controls and a lack of understanding of the rights of students and parents, especially over student directory information, result in more personally

identifiable information about students becoming public, increase the risk that students will become victims of identity theft, threaten the physical safety of some students, and allow for unregulated commercial use of student information.

(g) Schools and others that maintain personally identifiable information about students and others would greatly benefit from an authoritative source of privacy and security assistance focused on the risks that can affect the records they maintain. Students, parents, and others would also benefit.

Section 3. Definitions

(a) "Covered organization" means a school, a State agency that processes personally identifiable information for or from schools, and a contractor, grantee, or researcher that processes personally identifiable information for or from schools.

(b) "Personally identifiable information" means information about an individual processed by a covered organization, including any of the following:

(1) first and last name;

(2) home or other physical address, including street name and city or town;

(3) e-mail address;

(4) telephone number;

(5) social security number or other code or account number assigned to an individual, including a student identification number;

(6) IP address;

(7) fingerprint or photograph;

(8) any other identifier that permits the physical or online contacting of a specific individual;

(9) any representation of information that permits the identity of the individual to whom the information applies to be reasonably inferred by either direct or indirect means.

(c) "Processing" means with respect to personally identifiable information the collection, use, disclosure, maintenance, storage, erasure, or destruction of the personally identifiable information.

(d) "School" means any [public school, any non-public school of secondary education, any private

school, any charter school, any for-profit school, and any school of higher education].

(e) "Security" means administrative, physical, and technical safeguards for personal information or information systems containing personal information.

Section 4. Appointment and Qualifications.

(a) There is hereby created in the State [Department of Education] the Office of Chief Privacy Officer for Education.

(b) The Governor shall appoint the Chief Privacy Officer for Education, who must be qualified by training or experience in privacy, civil liberties, information technology, or information security, and who shall take office upon confirmation by a majority of the membership of the Senate and a majority of the membership of the Assembly.

(c) The Chief Privacy Officer for Education shall serve for a term of five years and may be reappointed to one additional term of five years.

(d) The Chief Privacy Officer for Education may continue to serve in office after the expiration of his or her term of office until a successor is appointed and confirmed.

(e) The Chief Privacy Officer for Education may not be removed from office except for neglect of duty or malfeasance in office.

(f) The Chief Privacy Officer for Education shall receive salary and benefits equivalent to [xxx].

Section 5. Functions

(a) The functions of the Chief Privacy Officer for Education include but are not limited to:

(1) promoting the implementation of fair information practices for privacy and security of personally identifiable information processed by covered organizations;

(2) providing direct or indirect assistance or advice on privacy and security matters to covered organizations, students, parents, school organizations, State agencies, the legislature, and others as the Chief Privacy Officer for Education deems appropriate;

(3) advising students, parents, and other individuals about options and actions that they can take to protect the privacy and security of personally identifiable information;

(4) making recommendations on privacy and security to the Legislature, Governor, Department of Education, Federal Department of Education, covered organizations, students, parents, and school organizations;

(5) conducting oversight or audits of privacy and security activities at covered organizations;

(6) preparing privacy impact assessments for activities affecting privacy or security at covered organizations, and commenting on privacy impact assessments prepared by others;

(7) publishing model privacy and security policies and best practices for covered organizations, including standards for –

(A) privacy impact assessments;
(B) minimizing the processing of personally identifiable information, including the retention of the information;
(C) anonymizing personally identifiable information;
(D) the maintenance of audit logs that record information on the use or disclosure of personally identifiable information;
(E) responding to security breaches and providing notification to affected individuals;
(F) the use and disclosure of directory information about students, including standards for schools that allow students and parents to opt-out of disclosures of directory information;
(G) privacy and security obligation that should apply when covered organizations outscource the processing of personally identifiable information;
(H) disclosure of information about student athletes, student award recipients, and other student accomplishments;
(I) access by officials of covered organizations to social networking sites maintained by students, parents, and other individuals;
(J) the use of cloud computing services;
(K) public notices that describe the processing of personally identifiable information by covered organizations;
(L) Sharing of personally identifiable information with other states, nonprofit organizations, education technology companies, content providers and developers; and
(M) use of personally identifiable information for research and statistical purposes by covered organizations and by others.

(8) cooperating with other States and with the Federal government on privacy and security matters;

(9) promoting or conducting voluntary and mutually agreed upon nonbinding arbitration and mediation of privacy-related or security-related disputes involving schools where appropriate;

(10) receiving complaints from parents, students, and other individuals concerning the processing of personally identifiable information by covered organizations and, within the limits of available resources, providing advice, information, and referrals in response to the complaints;

(11) providing or sponsoring training in privacy and security for covered organizations and others affected by this Act;

(12) preparing and distributing lesson plans and other materials that will allow teachers to

teach students about privacy and privacy rights;

(13) maintaining a public web page providing information and resources about privacy and security; and

(14) proposing legislation or commenting upon legislation pending before the Legislature that affects any activity within the scope of this Act.

(b) The Chief Privacy Officer for Education shall report directly to the [Commissioner of Education] and may report directly to the Governor and to the Legislature when the Chief Privacy Officer for Education deems it appropriate.

(c) The Chief Privacy Officer for Education shall submit an annual report directly to the [Legislature], Governor, [Commissioner of Education], and public, and may submit additional reports as the Chief Privacy Officer sees fit. The annual report shall include a summary of activities, recommendations, publications, and complaints received about privacy violations, and other matters.

Section 6. Powers

The Chief Privacy Officer for Education shall have the following powers:

(a) to access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by covered organizations that relate to privacy and security matters relevant to activities authorized under this Act;

(b) for any privacy or security matter relevant to activities authorized under this Act, to (1) conduct public hearings; (2) require by subpoena the production of records, reports, audits, reviews, documents, papers, recommendations, and other materials, and (3) compel the attendance of witnesses;

(c) to enforce a subpoena in any court of competent jurisdiction using counsel (1) hired by or otherwise available to the Chief Privacy Officer for Education; or (2) provided by the Attorney General or the [Secretary of Education].

(d) to administer to or take from any person an oath, affirmation, or affidavit, whenever appropriate in the performance of responsibilities under this Act;

(e) to review and comment upon any [State Department of Education] program, proposal, grant, or contract that involves the processing of personally identifiable information before the [Secretary of Education] begins or awards the program, proposal, grant, or contract;

(f) to hire employees and enter into contracts.

Section 7. Effective Date

This Act shall take effect 60 days after the date of enactment.

United States House of Representatives
Committee on Education and Labor

Hearing on
"How Data Can be Used to Inform Educational Outcomes"
April 14, 2010

Statement of Joel R. Reidenberg Professor of Law and Founding Academic Director Center on Law and Information Policy Fordham University School of Law
New York, NY

Good morning Mr. Chairman, Ranking Member, and distinguished members of the Committee. I would like to thank you for the invitation to testify today and to commend you for recognizing the importance of privacy protections in the development of databases of children's educational records.

My name is Joel Reidenberg. I am a Professor of Law and the Academic Director of the Center on Law and Information Policy ("CLIP") at the Fordham University School of Law. As an academic, I have written and lectured extensively on data privacy law and policy. Of relevance to today's hearing, I directed with Jamela Debelak, CLIP's Executive Director, the CLIP report "Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems" (Oct. 28, 2009) <http://law.fordham.edu/childrensprivacy>. I am a former chair of the Association of American Law School's Section on Defamation and Privacy and have served as an expert adviser on data privacy issues for the Federal Trade Commission, the European Commission and during the 103rd and 104th Congresses for the Office of Technology Assessment. I have also served as a Special Assistant Attorney General for the State of Washington in connection with privacy litigation. In appearing today, I am testifying as an academic expert and my views should not be attributed to any organization with which I am affiliated.

My testimony today draws on the Fordham study and I would like to make three points directly from it:

1. **States are warehousing sensitive information about identifiable children.**

2. **The Fordham CLIP study documents that privacy protections are lacking and rules need to be developed and implemented to assure that children's educational records are adequately protected.**

3. As part of basic privacy standards, strong data security is necessary to minimize the risks of data invasions, scandals and melt-downs from centralized databases of children's personal information.

My research focus on the treatment of K-12 educational records began in October 2006. As an elected member of the Millburn Township Board of Education in New Jeresey, I heard a speech by the state commissioner of education extolling the roll-out of the NJ SMART data warehouse later that fall. The NJ SMART program required our district to provide detailed, sensitive information about our school children on an identifiable basis to the state's central database. None of the commissioner's plans indicated any effort to focus data collection on truly necessary information, nor did they reflect any limitation on the purposes for use of the data once collected, nor did the plans appear to have any means for parents to check the accuracy of state-held information, and nor did the plans have any limitations on the length of storage. The only recognition that privacy might be affected by NJ SMART was an architecture that included data security mechanisms. As a Board member, I was disturbed that the state had given our district a mandate that would invade our children's privacy for ill-defined purposes in a way that appeared to put the district in clear violation of the Family Educational Rights and Privacy Act ("FERPA"). I was equally troubled that this database was established without public transparency and debate on the policy ramifications for children's privacy. Our Board and others we asked had not even heard about the program.

In delving further into the New Jersey program, it became apparent that New Jersey was part of a national trend to create state data warehouses of children's educational records driven by No Child Left Behind and more recently expanded by the American Recovery and Reinvestment Tax Act of 2009. The national trend similarly had emerged without public debate regarding privacy. As a result, we launched the Fordham CLIP study to determine what existed across the country at the state level, to assess whether states were protecting the privacy of the children's information in these databases and to make best practices and legislative reform recommendations as appropriate.

At the outset, I would like to stress that our study and I do not challenge the importance and legitimacy of data collection and use to better inform educational outcomes. Rather, I seek to highlight the critical need for policy makers to incorporate privacy rules in the planning and implementation of these systems so that the important and legitimate goals of educational accountability do not undermine privacy and so that the important and legitimate privacy concerns do not pose unnecessary obstacles to educational accountability.

1. States are warehousing children's sensitive personal information

The Fordham study found that most states have established state-wide databases of children's educational records. The information held at the state level is typically identified or identifiable to individual children because the databases use unique identifiers for each child and very few states use systems that establish a firewall to keep

the identity of individual students known only at the local level. One-third of the states track students through their social security numbers. In other words, most states are developing systems that centralize at the state level each individual child's information rather than transferring data aggregated by cohorts to the state level.

For a disturbing number of states such as Alabama, Arizona, Maryland, Nevada and Oklahoma, key information on the data warehouse programs including the types of data that were being collected and used were not publicly available. This means that state governments are conducting major data processing operations involving children's sensitive information essentially in secret from parents.

In states where information was publicly available on the data warehouse programs, the Fordham study found that states were collecting children's personal information to comply with NCLB reporting obligations such as test scores, race, ethnicity, gender, and disability status. However, the states were also collecting sensitive information well beyond NCLB reporting requirements. The following table gives some examples of the sensitive data collected by states.

Longitudinal Databases and Sensitive Data

- ***32% of states collect children's social security numbers***
- ***22% of states record student pregnancies***
- ***46% of states have a mechanism in place to track children's mental health, illness and jail sentences***
- ***72% of states collect children's family wealth indicators***

Source: Fordham CLIP Study, "Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems" (Oct. 28, 2009), p. 27

Many additional data elements included in the state databases do not appear to be collected for NCLB reporting purpose nor for core educational assessment purposes. Louisiana schools, for example, must report to the state the social security number of each child who is disciplined for the use of foul language in school.

Data warehouses appear to gather data for other goals like the delivery of social services. For example, Florida uses social security numbers to collect information about its K-12 children and collects the birth weight of a teenage mother's baby. While the

birth weight of a teenage mother's baby can be valuable information to anticipate social service needs, the decision to include this information as part of an educational record at the state level permanently linked to the teenager and the baby raises many privacy risks that need to be justified and balanced against the actual benefits for the mother and child. The following table illustrates some of these types of data found in the state data warehouses.

Examples of Other Sensitive Data
Collected by the States

- ***Birth order***
- ***Birth weight of a student's baby***
- ***Victim of peer violence***
- ***Medical test results***
- ***Parental education level***
- ***Mental health problems***
- ***Criminal history***

Source: Fordham CLIP Study, "Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems" (Oct. 28, 2009), p. 31

In developing data warehouses, the U.S. Department of Education has encouraged the use of interoperable data standards. Organizations, such as the Data Quality Campaign and the Standards Interoperability Framework Association, have significantly advanced the development of common data protocols. These common protocols are valuable to improve the efficiency of data collection and use. But, the use of interoperable data standards across state lines also means that the creation of a national database of children becomes a turn-key operation. Until the recent efforts of the Data Quality Campaign, basic privacy protections were not included as key components of the work on common data standards.

2. The Lack of Privacy Protection

The Fordham study showed that the state data warehouses of children's information typically lacked basic privacy protections and, often, were not in compliance with FERPA.

Existence of Key Privacy Protections

- **Only 18 states have detailed access and use restrictions**
- **Only 18 states require database users to enter into confidentiality agreements**
- **Only 10 states have data retention policies**
- **49 states make FERPA information accessible on the Internet, but for many the information is hard to find, vague or incomprehensible**

Source: Fordham CLIP Study, "Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems" (Oct. 28, 2009), p. 39

As a starting point, the states' lack of transparency for these databases is deeply troubling. Our research team had significant difficulty and was unable to find publicly available information on the data collected by many states. As far as parents are concerned, this means that state governments have created secret surveillance systems for their children. The non-transparent nature of these systems also means that state government can avoid public accountability for its treatment of children's personal information.

The technical architectures generally did not adequately seek to de-identify children's information at the state level. To the extent that outcome assessment can effectively be accomplished by examining cohorts at the state level, rather than individual children, there is no need for the state educational agency to have individual student records. The use of truly anonymous information would avoid privacy issues. However, we did not systematically see careful attention to architectures that established identity firewalls. Professors Krish Muralidhar and Rathindra Sarathy have demonstrated that re-identification of specific children from purportedly anonymous student information is already a problem in the context of public reporting on school performance.[1]

Data minimization, a basic privacy principle that collections of personal information should not be conducted as general fishing expeditions, is absent as a guiding policy for the state warehouses. The scope of sensitive children's information that is

[1] Krish Muralidhar & Rathindra Sarathy, "Privacy Violations in Accountability Data Released to the Public by State Educational Agencies," paper presented to the Federal Committee on Statistical Methodology Research Conference, Washington DC, November 2-4, 2009 available at: <http://gatton.uky.edu/faculty/muralidhar/EdPrivacyViolation.pdf> (last visited Apr. 9, 2010).

collected by states appears to be excessive with respect to the context and core educational purposes of the databases.

The state data warehouses generally did not have clear legal limitations on the purpose for which data could be accessed and used. Without purpose limitations, states, such as New Jersey, are in facial violation of FERPA. FERPA only permits local schools to report data to state agencies in identifiable format for "audit and evaluation" purposes. The lack of purpose limitations strongly suggests that states will begin a mission creep and use children's educational data for a multiplicity of purposes unrelated to assuring the educational performance of the state's schools. Most states also did not explicitly require state officials to agree to confidentiality before accessing student information.

The states by and large ignore data retention policies. The lack of storage limits means that a child's third grade peccadillo and youthful indiscretions will indeed become a "permanent record" since states store detailed disciplinary and social information, including in some instances if a child was the victim of bullying. The lack of storage limitations is a facial violation of FERPA as FERPA requires that data transferred to state authorities for audit and evaluation purposes not be retained longer than necessary to accomplish those permissible purposes. The lack of durational limits also undermines other important public policies. For example, the detailed disciplinary information collected on identified students, including involvement and convictions under the juvenile justice system will be held indefinitely as part of the "educational records" database. While the juvenile records are typically sealed and may be expunged when a minor reaches adulthood, the state's educational database without a data retention policy does not provide any such protection.

Many states outsource the data processing services for their data warehouses. While security and confidentiality provisions can be found in some of these contracts, the clauses are typically very circumspect with respect to the vendor's obligations. Vendor contracts are generally silent with respect to uses and retention of data by the vendor.

The Fordham CLIP study identified key privacy protections that need to be implemented for children's educational record databases:

- *States should implement a technical architecture to prevent access to identifiable information beyond the school officials who need to know*
- *States that outsource data processing should have comprehensive agreements that explicitly address privacy*
- *States should limit data collection to necessary information for articulated, defined purposes*
- *States should have specific data retention policies and procedures*
- *States should explicitly provide for limited access and use of the children's data*
- *States should provide public notice of state data processing of children's information*

3. Strong data security is necessary to minimize the risks of data invasions, scandals and melt-downs from centralized databases of children's personal information.

In addition to basic privacy protections, data security is critical when information relating to identifiable children is centralized at the state level. Data security measures do not address the essential policy decisions for privacy protections like data minimization, purpose limitations, and defined storage periods. But, data security measures play a critical role in the implementation of privacy protections specifically with respect to the prevention of unauthorized access, use and disclosure of personal information.

The centralization of children's information at the state level increases the risks and scope of loss from security incidents. The centralization means that data security breaches will be on a larger scale than if data were held solely at the local level. For example, according to the Congressional Research Service up to 1.4 million residents of Colorado had their names, social security numbers and birth dates compromised when a database from the state department of human services was stolen from a private contractor in Texas.[2]

It is inevitable that security of the children's information will be compromised. The experiences in the financial services sector that have been revealed by data security breach notification laws reflect the magnitude of this risk. Despite the deployment of significant resources and the economic incentive for banks to avoid liability, the number of compromised credit cards in the United States is staggering. The Heartland Payment Systems breach alone in 2009 involved more than 100 million credit and debit card transactions. State departments of education have neither the resources nor the same high level of incentive to protect children's information to the degree that the financial services sector does.

The substantial security risks to children's educational records in data warehouses can be illustrated by a few examples:

- **Data spills** occur when school or state officials fail to assure adequate access controls and encryption for student records

[2] CRS Report for Congress, Data Security Breaches: Context and Incident Summary, p. 62 (May 7, 2007) available at: <http://www.fas.org/sgp/crs/misc/RL33199.pdf>

Recent Data Spills

Catawba County, NC: names, test scores and SSNs of school children exposed on the web (2006)
Nashville, TN: personal information of 18,000 students and 6,000 parents released on the internet from state data warehouse program (2009)
100 Public Schools and Local Government Entities: FTC warns that their files of personal information can be found freely on the web with P2P technology (2010)

- **Hackers** gain access to data when it is insufficiently protected

Hacking Cases

Churchill High School, Potomac, MD: students hacked school records system to alter data
Haddonfield High School, Haddonfield, NJ: students hacked into school records database

- **Data loss and theft** compromise educational records when they are insufficiently protected

Loss and Theft Cases

Broward County, FL: ChildNet lost personal information on adoptive and foster families including SSNs, passport numbers, credit data, drivers' license information
Chicago Public Schools, IL: lost personal information on 40,000 teachers and employees when 2 laptops stolen
Colorado: lost health records on 1,600 named, autistic children when laptop stolen from state employee's home (2005)
Greenville County School District, NC: lost personal information on 100,000 students and staff when district laptops auctioned off

- **Data spys and voyeurs** who are internal employees with access privileges abuse their access to personal information for personal gain

Spying and Voyeur Cases

UCLA Medical Center: hospital worker sells celebrity patient information to media
IRS: tax agent in Kentucky convicted for spying on 200 actors and sports figures

Strong data security for children's educational records is, thus, essential. Four critical features for a strong security system are:

- *States should avoid the storage of identifiable information whenever possible.*
- *States should use state-of-the art encryption to protect children's data*
- *States should have robust access control and use authorization policies in place*
- *States should, like the IRS, maintain audit logs that track system use to detect intrusions and police internal misuse*

Conclusion

The Fordham CLIP Study recommends several measures that I believe Congress should consider as a condition of continued federal funding of state data warehouses of children's information:

1) **Require that states articulate through statute or regulation the justification for the collection of each element of identifiable information.** This assures that the legitimate uses are transparent and sufficiently compelling to warrant the privacy trade-offs.
2) **Require that states define specific data retention limitations that are clearly linked to the specific purposes for which the data is originally collected.** This reduces the risks of data spills, protects against mission creep, and
3) **Require that states adopt an oversight mechanism for the collection and use of children's educational data.** 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.

Biography

Joel R. Reidenberg is Professor of Law and the Founding Academic Director of the Center on Law and Information Policy at Fordham Law School. He is a former Associate Vice President for Academic Affairs and Associate Chief Academic Officer of Fordham University and a former President of the University's Faculty Senate (the governing body of the university-wide faculty).

Professor Reidenberg is an expert on information technology law and policy. His published books and articles explore both information privacy law as well as the regulation of the internet. He teaches courses in Information Privacy Law, Information Technology Law, and Intellectual Property Law. He has held appointments as a visiting professor at the Université de Paris 1 (Panthéon-Sorbonne), at the Université de Paris V (René Descartes) and at AT&T Laboratories - Public Policy Research .

Professor Reidenberg has served as an expert adviser on data privacy matters for the U.S. Congress, the Federal Trade Commission and the European Commission. He also served as a Special Assistant Attorney General for the State of Washington in connection with privacy litigation. Reidenberg has chaired the Section on Defamation and Privacy of the Association of American Law Schools (the academic society for American law professors) and is a former chair of the association's Section on Law and Computers.

Prior to coming to Fordham, Reidenberg practiced law in Washington, DC with the international telecommunications group of the firm Debevoise & Plimpton.

Professor Reidenberg received an A.B. degree from Dartmouth College, a J.D. from Columbia University, and both a D.E.A. droit international économique and a Ph.D in law from the Université de Paris -Sorbonne. He is admitted to the Bars of New York and the District of Columbia.