United States House of Representatives
113th Congress, 2nd Session

Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

and

Committee on Education and the Workforce
Subcommittee on Early Childhood, Elementary and Secondary Education

Hearing on
"How Data Mining Threatens Student Privacy"
June 25, 2014

Statement of Joel R. Reidenberg
Stanley D. and Nikki Waxberg Chair and Professor of Law
Founding Academic Director, Center on Law and Information Policy
Fordham University
New York, NY

Good morning Chairman Meehan, Representative Clarke, Chairman Rokita, Representative Loebsach and distinguished members of the Subcommittees. I would like to thank you for the invitation to testify today on this critical privacy issue for our nation's school children.

My name is Joel Reidenberg. I am here today as an academic expert on student information and privacy. I hold the Stanley D. and Nikki Waxberg Chair at Fordham University where I am a professor of law and the Academic Director of the Center on Law and Information Policy ("Fordham CLIP"). I am also just finishing my term as the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton University.

As a law scholar, I have written and lectured extensively on data privacy law and policy. I am a member of the American Law Institute where I serve as an Adviser to the *Restatement of the Law Third on Information Privacy Principles*. 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.

Of relevance to today's hearing, I directed the research study "Privacy and Cloud Computing in Public Schools" (Dec. 2013) ["Fordham CLIP Study"] that provides a benchmark analysis of the processing of student information by online vendors and that also documents the current legal risks surrounding student privacy.[1] Two members of the Fordham CLIP research team, N. Cameron Russell, Fordham CLIP's Executive Director, and Thomas B. Norton, Fordham CLIP's Privacy Fellow, accompany me here today.

In appearing today, I am testifying as an academic expert and my views should not be attributed to any organization with which I am or have been affiliated.

My testimony today draws specifically from the Fordham CLIP Study. I will address a number of our key findings.

1. **Schools are uniformly transferring vast amounts of student information to online third parties for many varied purposes.**

School districts across the country are rapidly embracing evolving online technologies to meet data-driven educational goals, satisfy reporting obligations, realize information technology cost-savings, and take advantage of new instructional opportunities.

The Fordham CLIP Study found that 95% of public schools in the United States use online services that involve the transfer of student information to third parties. Schools use these services for a myriad of purposes that the Fordham CLIP Study categorized as follows:

- Data analytics functions
- Student reporting functions
- Classroom functions
- Guidance functions
- Special school functions (e.g., transportation services)
- Hosting, maintenance, and backup functions[2]

[1] Joel R. Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier, Daniela Alvarado, *Privacy and Cloud Computing in Public Schools* (Dec. 2013) available at http://law.fordham.edu/k12cloudprivacy [hereinafter "Fordham CLIP Study"] I also directed an earlier study, *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems* (Fordham CLIP: Oct. 28, 2009) http://law.fordham.edu/childrensprivacy and testified on that work in a hearing before the House Committee on Education and Labor during the 111th Congress.

[2] Fordham CLIP Study, at pp. 17-18

These online services involve the collection and transfer of enormous quantities of student information to third party commercial organizations including school records, homework essays, fitness profiles, and even lunchroom purchases.

2. Federal education privacy law fails to protect student information in a vast range of commercial computing services used by schools.

Three federal privacy statutes address student information that may be collected by and from schools: the Family Educational Rights and Privacy Act of 1974[3] ("FERPA"), the Children's Online Privacy Protection Act[4] ("COPPA"), and the Protection of Pupil Rights Amendment[5] ("PPRA").

FERPA is the oldest and best-known educational privacy statute. The statute seeks to provide confidentiality to student data, but only covers "educational records" in a very narrow sense (e.g., transcripts).[6] The statute also specifically exempts "directory information," including a student's name, address, date of birth, telephone number, age, sex, and weight from confidentiality obligations.[7] Most significantly, FERPA was written forty years ago before public schools had computers, let alone internet access. As acknowledged by the Department of Education, the applicability of FERPA to typical online school services is questionable at best.[8]

The other statutes, COPPA (addressing parental consent for online collection of data directly from children younger than 13) and PPRA (primarily addressing the use of data collected from in-school surveys and some marketing activities), similarly suffer from significant protection gaps in the context of cloud computing, that the Fordham CLIP Study explains.

Many cloud services used by schools are, thus, completely outside the protections of these statutes. For example, when a middle school uses a cloud service provider to offer young teens self-assessment tests that give scores to their language or math levels, those scores will not likely be protected by the federal statutes: they are not FERPA "educational records" because they are not used for the middle schooler's transcript grade, they do not require COPPA parental consent, and they fall outside the PPRA categories of protection. Thus, there is no statutory obligation of confidentiality.

---

[3] 20 U.S.C. § 1232g
[4] 15 U.S.C. §§ 6501-6506
[5] 20 U.S.C. § 1232h
[6] See Owasso Independent School District v. Falvo, 534 U.S. 426 (2002)
[7] 20 U.S.C. § 1232g(a)(5)(A)
[8] Dept. of Educ., Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, PTAC FAQ3 (Feb. 2014) http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services (the Department wrote: "Is student information used in online educational services protected by FERPA? It depends.")

Another example comes from special school functions: schools are now using third-party online service providers to manage payments for the school cafeteria. When a child buys a meal in the school cafeteria, the information about the child's eating habits will not have privacy protection.

Another important point to note is that FERPA does not apply to vendors. By its terms, FERPA only applies to educational agencies and institutions that are recipients of federal funds.[9] FERPA does not provide a private right of action,[10] and the only sanction available under FERPA is the denial of federal educational funds by the Department of Education. The Department has never issued such an order. Thus, under federal law, legal protection for student privacy will only come from the contractual terms in agreements between schools and vendors.

States, however, are increasingly concerned about the commercial sale of student information. According to recent reports, over 30 states across the country have bills at various stages of enactment to address student privacy online. These bills do not generally address the full range of issues and would establish different protections for students in different states.

3. The Fordham CLIP study documents that schools routinely relinquish student privacy when they contract for online services and parents are kept in the dark.

In the absence of statutory rights, schools can protect student privacy through their contracts with online service providers. The Fordham CLIP Study , however, demonstrates that contracts between schools and vendors often fail to establish legal rights that protect student information. Schools essentially relinquish their students' privacy in the cloud. And, at the same time, schools routinely fail to inform parents that their children's data is sent to third-parties.

Among the findings, the Fordham CLIP Study reported that:

- **Technology governance controls are absent:** 20% of school districts have no policies on the vetting and adoption of information technology services by teachers and staff.
- **Transparency is missing:** 75% of districts did not inform parents that their children's data was being released to online service providers, and districts do not readily make their agreements publicly accessible.
- **Legal compliance is not working:** COPPA is frequently ignored; FERPA notices are rare.
- **Contract practices are disturbing**: Over 75% of the agreements fail to specify a legitimate purpose for processing student data, vendors are routinely able to

[9] 20 U.S.C. § 1232g(a)
[10] Gonzaga Univ. v. Doe, 536 U.S. 273 (2002)

modify the privacy terms on a unilateral basis, and schools fail to keep adequate documentation of their contracts.

- **Student data may be sold for advertising and marketing:** Fewer than 7% of agreements explicitly prohibit the sale or marketing of student information, though higher percentages of agreements have general restrictions on re-disclosure. Without a contractual prohibition, vendors are free to sell the student information.
- **Data security protections are poor:** 40% of hosting agreements, like many other categories, fail to require any data security and, depending on the type of service, 33% or more of the agreements fail to require the deletion of student information at contract termination.[11]

These findings present a very disturbing set of risks to the privacy of our nation's student information. A permanent record may now indeed follow a child from elementary school through adulthood. For example, the company ConnectEdu held data on over 20 million students and offered a product called K12 Early Warning Indicator.[12] The product sought to label students with the goal of identifying and helping at-risk students. But, the lack of privacy protection means that the label may now follow the child indefinitely. Worse still, the company is now in bankruptcy and the Federal Trade Commission had to make a special filing in the hope that it could persuade the bankruptcy judge not to sell off to the highest bidder all the student data held by the bankrupt company,[13]

Similarly, student data becomes fuel for commercial uses. In some contexts, such as those involving classroom functions, 25% of the school contracts involved no financial payments. This likely means that these vendors are monetizing the student information to fund the services they provide. In other words, school districts are paying for services with their students' privacy rather than cash. This was dramatically illustrated by disclosures in the law suit against Google for its scanning of student email. Originally, Google represented to educational institutions that it did not scan student email for commercial advertising.[14] As it turned out, Google was profiling students based on their

---

[11] See Fordham CLIP Study, Executive Summary, pp. 1-2.

[12] See ConnectEdu, About Us http://connectedu.com/about-us (stating the company had data on 20 million 'registered learners'); ConnectEdu, What does K12 Early Warning do for you, http://207.127.11.51/products-k12earlywarning-features.html ("locate students at risk")

[13] See Federal Trade Commission Letter From Jessica L. Rich, Director of the Bureau of Consumer Protection, Filed With the Bankruptcy Court for the Southern District of New York -- in In re ConnectEDU, Inc., No. 14-11238 (Bankr. S.D.N.Y.)(May 22, 2014) http://www.ftc.gov/system/files/documents/public_statements/311501/140523connectedu commltr.pdf

[14] See Jeff Gould, Google admits data mining student emails in its free education apps, SafeGov.Org (Jan. 31., 2014) http://safegov.org/2014/1/31/google-admits-data-mining-student-emails-in-its-free-education-apps (quoting a pre-2013 Google FAQ saying "note that there is no ad-related scanning or processing in Google Apps for Education")

email.[15] In a policy change announced on April 30, 2014, Google said that it would no longer "collect or use student data in Apps for Education services for advertising purposes."[16] Google remains silent, however, on scanning email and profiling student users for other commercial purposes and partnerships with education technology companies. Google is not alone. The other companies that offer education technology products without fees are or will be trading on student privacy.

4. Without strong and effective privacy protections for student information, data-driven educational policies will fail and parents will oppose new instructional methods.

The responsibility for placing student privacy at risk through these observed practices is complex. Federal laws such as the No Child Left Behind Act and the American Recovery and Reinvestment Act of 2009 required schools to create and report detailed student information. Innovations in technology and incentives for data mining create new demands for student information. Yet, at the same time, education privacy laws have not been modernized to keep up, and our research revealed that schools were not equipped to address these issues effectively.

Data collection and use to inform and improve student learning is critical to making education successful in the United States. But so is the long-term health of our children's privacy. More often than not, school districts poorly understood the data transfers and privacy implications of the online services they use.[17] Other than the largest districts with legal offices, few had either the expertise or the ability to negotiate contract terms that were drafted by vendors.

As a result, today's status quo is an unstable and contentious environment for education technology. The recent failure of inBloom, a $100 million venture to develop a platform for education data, demonstrates that privacy risks will shut down programs when public concerns are not addressed effectively.[18] If privacy is not adequately and transparently

---

[15] See Michele Molnar, Google Abandons Scanning of Student Email, Education Week, Apr. 20, 2014, http://blogs.edweek.org/edweek/marketplacek12/2014/04/google_abandons_scanning_of_student_email_accounts.html

[16] Protecting students with Google Apps for Education, Apr. 30, 2014 http://googleenterprise.blogspot.com/2014/04/protecting-students-with-google-apps.html

[17] See Fordham CLIP Study, p. 15 (describing districts' lack of knowledge of their own agreements); Stephanie Simon, Data mining your children, Politico, May 15, 2014 http://www.politico.com/story/2014/05/data-mining-your-children-106676.html ("school administrators ... don't know which digital tools individual teachers are using in the classroom.")

[18] See Benjamin Herold, inBloom to shut down amid growing privacy concerns, Eduation Week, Apr. 21, 2014 http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html

addressed, parents will oppose the use of education technologies for fear of their children's safety.

Strong and effective privacy protections for student information are essential for data-driven educational policies to succeed.

Recommendations

There are a number of steps Congress can take to restore and assure the privacy of student information:

1) **Modernize FERPA to protect and limit the use of all student information whether held by schools or vendors—including a prohibition on non-educational uses of student information and graduated enforcement remedies such as private rights of action.**

2) **Require that the processing of student data under any federally financed educational program be prohibited unless there is a written agreement spelling out the purposes for the processing, restricting the processing to the minimum amount of data necessary for those purposes, restricting the processing to permissible educational uses, mandating data security, requiring data deletion at the end of the contract, and providing for schools' audit and inspection rights with respect to vendors.**

3) **Require that states adopt an oversight mechanism for the collection and use of student data by local and state educational agencies. A Chief Privacy Officer in state departments of education is essential to provide transparency to the public, assistance for local school districts to meet their privacy responsibilities, and oversight for compliance with privacy requirements.**

4) **Provide support to the Department of Education and to the research community to address privacy in the context of rapidly evolving educational technologies, including support for a clearing center to assist schools and vendors find appropriate best practices for their needs.**

Thank you again for the opportunity to participate in this hearing and for your consideration of my testimony.

Biography

Joel R. Reidenberg holds the Stanley D. and Nikki Waxberg Chair at Fordham University where he is a professor of law and the Founding Director of the Center on Law and Information Policy ("Fordham CLIP").

Professor Reidenberg is an expert on information technology law and policy. He is an elected member of the American Law Institute and serves as an Adviser to the *ALI Restatement of the Law Third on Information Privacy Principles* 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 served as the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton University and 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.