United States House of Representatives
114th Congress, 1st Session

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

Hearing on
"How Emerging Technology Affects Student Privacy"
February 12, 2015

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 Rokita, Ranking Member Fudge and distinguished members of the Committee. I would like to thank you for the opportunity to testify today on emerging education technologies and their effects on the privacy of our nation's school children.

My name is Joel Reidenberg. I am a law professor at Fordham University where I hold the Stanley D. and Nikki Waxberg Chair in Law and a visiting lecturer at Princeton. I am also the founder and director of the Fordham Center on Law and Information Policy ("Fordham CLIP"). As an academic, I have written and lectured extensively on data privacy law and policy and 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*. Of particular relevance to today's hearing, I directed the Fordham CLIP research studies on *Privacy and Cloud Computing in Public Schools*" (Dec. 12, 2013) http://law.fordham.edu/k12cloudprivacy, and on *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems* (October 2009) http://law.fordham.edu/childrensprivacy/. I also supervised the Fordham CLIP *Privacy Handbook for Student Information Online: A Toolkit for Schools and Parents,* http://law.fordham.edu/center-on-law-and-information-policy/34710.htm that was just released last week. On a direct practical level, I served for five years as an elected member of my local school board where I chaired the Board's Program Committee.

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

I would like to focus my testimony on the need to modernize federal educational privacy law to meet the challenges of today's educational technologies. I will place a particularly emphasis on the Family Educational Rights and Privacy Act of 1974[1] ("FERPA").

Education Technology, Schools and Data Use

Today, local schools are uniformly transferring vast amounts of student information to state educational agencies and to online third parties for many varied purposes.

At the state level, the enactment of *No Child Left Behind* established new school reporting obligations that increased data collections about individual children by state education departments. Over the ensuing years, the states created longitudinal databases known as State Longitudinal Data Systems ("SLDS") to track educational progress and often relied on private education technology vendors to provide hosting and analytic services. These SLDS collect and process extensive information about individual children and are designed using common data standards so that links can be made between state systems.[2]

At the local level, school districts across the country are rapidly embracing evolving online technologies to meet data-driven educational goals, satisfy their reporting obligations, realize information technology cost-savings, and take advantage of new instructional opportunities. These educational technologies serve many different functions including data analytics, student performance reporting, classroom and learning support, career guidance support, school bus route planning, and server hosting.[3] These online educational 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. In essence, most schools across the country outsource their children's data.

Outdated Education Privacy Law

Federal educational privacy law has failed to keep up with the developments in the use of student data and fails to protect the privacy of student information in a range of commercial computing services used by states and schools.

---

[1] 20 U.S.C. § 1232g

[2] See Joel R. Reidenberg, Jamela Debelak, et al. *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/ [hereinafter "Fordham CLIP 2009 Study"]

[3] Joel R. Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier & Daniella Alvarado, *Privacy and Cloud Computing in Public Schools*" (Fordham CLIP: Dec. 12, 2013) http://law.fordham.edu/k12cloudprivacy, [hereinafter "Fordham CLIP 2013 Study"], at pp. 17-18

Three federal privacy statutes address student information that may be collected by and from schools: 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. FERPA was enacted over forty years ago when student records were confined to file cabinets in the principal's office. The statute is essentially a confidentiality law that was designed to protect students' paper files. When FERPA became law in 1974, computers did not exist in schools and internet access was decades away. Consequently, FERPA does not function as a complete fair information practice statute for student information.

COPPA focuses on one particular issue: the online collection of personal information directly from children younger than 13 years old without parental consent. And, the PPRA primarily addresses the use of certain types of data collected from in-school surveys as well as some marketing activities.

Collectively, these three statutes miss the wide-ranging scope and scale of the use of student information through emerging educational technologies. As a result of high profile data sharing programs such as those proposed through inBloom[6] and revelations about the use of school data in commercial products such as the Google Apps for Education,[7] many states have explored new privacy requirements for student information. These requirements generally focus on prohibitions related to advertising and marketing uses of information gathered about school children. Many other concerns remain such as parental access and consent to the use of children's data, the legitimacy of non-marketing commercial uses of school data, data security and the sheer volume of data gathering programs.

Modernizing FERPA to meet today's needs

Without an adequate set of privacy protections for student information online, our children's privacy will be compromised and innovative education technologies and programs will face justifiable parental skepticism and opposition. We have already seen these effects with the dissolution of inBloom as a result of strong opposition related to

[4] 15 U.S.C. §§ 6501-6506
[5] 20 U.S.C. § 1232h
[6] 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
[7] 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

privacy[8] and with the failure of ConnectEdu to respect the conditions of student privacy in its bankruptcy proceeding.[9]

FERPA desperately needs to be updated in order to assure student privacy in the 21st Century and to enable the development of robust educational programs that take full advantage of educational technologies.

Five areas in FERPA need to be addressed:

1. **Update the definition of "Educational Record"**

FERPA covers "educational records" in a very narrow sense and contemplated only those records that were originally kept in central administration files such as transcripts.[10] The statute also specifically carves out an exemption for "directory information" including a student's name, address, date of birth, telephone number, age, sex, and weight.

The 1974 definition and the directory information exclusion no longer make sense in 2015. Much of the data gathered and used in the context of online services will be outside the scope of the existing definition. For example, metadata gathered from a learning app used by a child in school that was then compiled to create a profile of the child for content delivery would not be an "educational record" and would fall outside the bounds of FERPA. Similarly, information developed by a school's transportation company identifying the street corners where 6th graders wait to take the school bus would fall outside FERPA and could be disclosed for advertising purposes and even possibly disclosed to non-custodial parents. Likewise, a child's homework assignment saved or shared with a teacher on a third-party service would not be an "educational record" and would not protected by FERPA.

For meaningful protection of student privacy in this environment, FERPA needs to encompass any information gathered about children for educational and school related uses. This would include profiles, whether or not identified to specific students, if those profiles will have an effect on the child's education or school related services.

2. **Update FERPA to apply to vendors**

Currently, FERPA does not apply directly to vendors. By its terms, FERPA only applies to educational agencies and institutions that are recipients of federal funds.[11] When schools and state agencies use third-party vendors, the schools and agencies have compliance obligations, but the vendors do not. The vendor's only legal obligations

[8] See Herold, *supra note* 6.
[9] See Michelle Molnar, Millions of Student Records Sold in Bankruptcy, Education Week, Dec. 10, 2014, http://www.edweek.org/ew/articles/2014/12/10/millions-of-student-records-sold-in-bankruptcy.html
[10] See Owasso Independent School District v. Falvo, 534 U.S. 426 (2002)
[11] 20 U.S.C. § 1232g(a)

derive from their contracts with those schools and agencies.[12] Fordham CLIP's research demonstrated that typical contracts and SLDS programs have not adequately protected student information and, at the local level, schools are poorly equipped to address the vendor contracts.[13] While many responsible vendors are committing to protect student privacy through the Future of Privacy Forum's K-12 Student Privacy Pledge[14], the pledge is not an adequate substitute for meaningful legal protection applicable to all industry participants.

If FERPA is to cover adequately the ecosystem of student information, the statue must apply to all participants. The importance of this direct applicability is illustrated by a new trend among some ed tech companies to market products directly to teachers such as online gradebooks.[15] These marketing efforts are designed to bypass school administrators. As a result, these vendors are, in effect, soliciting teachers to violate FERPA because the teachers will generally not have the legal authority to enter into contracts for the transfer of the district's student data. While the Federal Trade Commission might be able to bring a deceptive practice claim, as a policy matter FERPA should address vendors directly.

3. Update FERPA to address "educational uses"

FERPA's original focus was on confidentiality and parental access to educational records. Now that student information is more extensive and the analysis of that data is more critical to the development of innovative learning tools, FERPA needs to provide clear parameters for legitimate educational uses of student information. FERPA should define permissible "educational uses" or "educational purposes" for student information and prohibit other uses without parental consent.

This approach is not new in American privacy law. The Fair Credit Reporting Act ("FCRA"), for example, is a permissible purpose statute. The law limits the use of consumer reports without consent to specifically defined purposes.[16] The FCRA's approach was very successful and has been widely recognized as a key factor in the development of a robust and fairer consumer credit market in the United States. For the education sector, there now needs to be a conscious public choice about the legitimacy of how information is gathered and used when the data comes from children in school.

---

[12] While under FERPA the Department of Education may bar a school from using federal funds to contract with a particular vendor, this indirect applicability is rare and cumbersome. See 20 U.S.C. 1232g(b)(4)(B).

[13] *See* Fordham CLIP 2013 Study, *supra note* 3; Fordham CLIP 2009 Study, *supra note* 2.

[14] See Future of Privacy Forum K-12 Student Privacy Pledge, http://studentprivacypledge.org/ (109 companies have signed the pledge as of Feb. 9, 2015)

[15] Stephanie Simon, Data mining your children, Politico, May 15, 2014 http://www.politico.com/story/2014/05/data-mining-your-children-106676.html

[16]

As a parent and former school board member, I do not believe that public schools should be used to gather students' information for private commercial gain or used to barter their children's information as products for third-party gain. Google, for example, has waived using student information mined from Google Apps for Education for advertising purposes.[17] But, what about data mining students' homework assignments or teacher interactions to profile the students and then use or sell those profiles to skew search engine results or modify delivered content? I believe that such types of commercial practices are not legitimate educational uses of student information and should be proscribed.

For educational privacy to be protected effectively by FERPA, the statute needs to specify that student information gathered online may only be used to provide direct educational benefits to the child whose information is used. Because the educational legitimacy of particular data collections and uses will often be contextually driven, FERPA also needs to have a safe harbor mechanism that will enable the Department of Education, state agencies and local schools to define the educational appropriateness of particular types of online practices.

By specifically enumerating legitimate educational uses and creating a safe harbor mechanism, I believe many of the complex issues related to the status of a data recipient such as whether a third party qualifies as a "school official" can be streamlined and resolved.

4. Expand FERPA to cover additional key information practices

FERPA includes important transparency requirements for student information. Parents have a right of access to their children's educational records held by educational agencies and institutions. This transparency needs to extend to any organization processing student information. Like the credit reporting system, families should be able to know who has their children's data and they should have the right to seek correction of inaccurate information.

In connection with transparency, processors of student information should be accountable to families regarding the identity of organizations to whom student information was disclosed. Credit reporting agencies must disclose to the consumer the identities of recipients of the consumer's credit report. Families deserve the same transparency for their children's information.

Another key information practice is data security. FERPA does not include any data security or breach notification obligation and a disturbingly large number of school

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

contracts with vendors fail to include security obligations or requirements.[18] With major security breaches occurring on an almost daily basis and with reported failures by education technology services to implement even minimal security,[19] student information needs legal protection that includes security and breach notification obligations.

5. Update FERPA enforcement remedies and oversight

The only sanction available under FERPA is the denial of federal educational funds by the Department of Education. This is a "nuclear option" and, to date, the Department has never issued such an order. FERPA needs to have a graduated range of remedies and broader enforcement capabilities, including fines and enforcement by the Federal Trade Commission and the state attorneys general along with the Department of Education.

The lack of a private right of action under FERPA means that victims and their families have no redress or remedy for the violation of a child's privacy.[20] For basic fairness, families should have a direct means of redress when their children's privacy is violated.

Lastly, FERPA confers guidance and oversight to the Department of Education that has a poorly funded office by comparison to the Office of Civil Rights in the Department of Health and Human Services where the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) are enforced.[21] FERPA can be more effective if Congress enhances the Department of Education's capacity to provide guidance and oversight. Likewise, educational privacy would be better served under FERPA if Congress were to encourage the states to create Chief Privacy Officer roles to provide local guidance through the respective state departments of education.

Recommendation

Congress can no longer wait to reform federal educational privacy rights. Congress should modernize FERPA to:

---

[18] In 2013, a Fordham CLIP study found that 40% of school data hosting agreements failed to require any data security and in other categories of services 33% or more of the agreements failed to require the deletion of student information at contract termination. See Fordham CLIP 2013 Study*, supra note 3*, Executive Summary, pp. 1-2.

[19] See Natasha Singer, Uncovering security flaws in digital education products for school children, NY Times, Feb. 9, 2015, p. B1 www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html

[20] Gonzaga Univ. v. Doe, 536 U.S. 273 (2002)

[21] For an interesting discussion of government agency privacy oversight activity, *see* Robert M. Gellman, *Who is the more active privacy enforcer: FTC or OCR*?, Concurring Opinions, Aug. 23, 2013, http://concurringopinions.com/archives/2013/08/who-is-the-more-active-privacy-enforcer-ftc-or-ocr.html

- **Protect all student information and not just "educational records" as conceived in 1974**
- **Apply directly to vendors**
- **Authorize the use of student information for specified educational uses and prohibit non-educational uses of student information**
- **Expand transparency obligations and add data security requirements**
- **Provide a range of enforcement remedies**
- **Encourage states to create Chief Privacy Officers**

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 has taught 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), Sciences Po-Paris 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.