Good morning Madame Chairwoman, Mr. Vice Chairman, Delegate Kaiser, and distinguished members of the Committee.

My name is Joel Reidenberg. I am the Microsoft Visiting Professor of Information Technology Policy at Princeton University this year and the Stanley D. and Nikki Waxberg Chair in Law at Fordham University. At Fordham, I also founded and direct the Center on Law and Information Policy (“Fordham CLIP”). As a scholar, I have written and lectured extensively on data privacy law and policy. Of relevance to today’s hearing, I directed the Fordham CLIP research study on “Privacy and Cloud Computing in Public Schools” (Dec. 12, 2013) http://law.fordham.edu/k12cloudprivacy (“Fordham CLIP Study”) and have testified before the US Congress on educational privacy issues.

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 thank you for your leadership in holding this hearing today and for Delegate Kaiser’s invitation to participate in this session.

My testimony this morning will focus on the need for HB 607 and make four points that draw from the Fordham CLIP Study which I would be happy to have included in the record:

1. Schools are uniformly using cloud services and transferring vast amounts of student information to online third parties.

2. Federal education privacy law does not protect student information in a vast range of commercial computing services used by schools

3. Schools typically relinquish student privacy when they contract for online services

4. HB 607 addresses a critical lack of privacy protection for school children’s information
1. **Schools are uniformly using cloud services and transferring vast amounts of student information to online third parties.**

Virtually every public school in the United States uses cloud computing services for data-driven educational planning, reporting obligations, teaching opportunities and cost savings. 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

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

2. **Federal education privacy law does not 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\(^1\) (“FERPA”), the Children’s Online Privacy Protection Act\(^2\) (“COPPA”) and the Protection of Pupil Rights Amendment\(^3\) (“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 such as transcripts.\(^4\) 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.

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

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

\(^1\) 20 U.S.C. § 1232g  
\(^2\) 15 U.S.C. §§ 6501-6506  
\(^3\) 20 U.S.C. § 1232h  
young teens self-assessment tests that give scores to their language or math levels, those scores will not 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. 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.

3. **Schools typically relinquish student privacy when they contract for online services**

In the absence of statutory rights, schools can protect student privacy through their contracts with cloud service providers. However, the Fordham CLIP Study demonstrates that the contracts between schools and vendors of cloud services fail to establish legal rights that protect student information. Schools essentially relinquish their students’ privacy in the cloud.

Among the findings, the Fordham CLIP Study reported that:

- 20% of school districts have no policies on the vetting and adoption of information technology services by teachers and staff
- Parents are not informed that schools send their children’s data to cloud service providers
- Over 75% of the agreements fail to specify a legitimate purpose for processing student data
- 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
- Vendors are routinely able to modify the privacy terms on a unilateral basis
- 40% of hosting agreements, like many other categories, fail to require any data security
- No less than 1/3rd of the agreements fail to require the deletion of student information at contract termination

More often than not, school districts appeared to understand poorly the data transfers and privacy implications of their cloud services and had neither the expertise nor the ability to negotiate contract terms that were drafted by the vendors.

4. **HB 607 addresses a critical lack of privacy protection for school children’s information**

HB 607 is tailored to address and solve two critically important privacy problems for student data transferred by schools to cloud service providers.
First, HB 607 seeks to require that schools and service providers set out in writing the purpose of services that will involve student information. This is a vitally important element to properly authorize the transfer of student information and it is essential for public transparency and accountability.

Second, HB 607 seeks to ban the commercialization of student data gathered through schools. The Fordham CLIP Study found that over 25% of cloud services for classroom functions were offered to schools without a financial charge. This means that the schools are, in effect, paying for the services with their students’ privacy. A national poll released last month by Common Sense Media reported that approximately 75% of Americans believe the sale of students’ private information to advertisers should be illegal and that the use of students’ online habits and searches in schools should not be used for profiling or target advertising. HB 607 would stop these practices.

HB 607 is an important step for the protection of student information against commercial, secondary use of private information. However, it does not address all of the disturbing shortcomings that are found in school cloud service arrangements.

Additional future steps that I urge the General Assembly to consider are:

- A requirement that school districts have governance policies that spell out the vetting and approval process for the adoption of information technologies in district schools including appropriate training for teachers and staff
- A requirement that agreements mandate appropriate levels of data security
- A requirement that cloud service providers be subject to compliance audits and inspections
- An enforcement mechanism through private rights of action against schools and cloud service providers for violations
- The establishment of a Chief Privacy Officer in the state department of education to assist local districts address these issues
- Support for ongoing research to address privacy in the context of rapidly evolving educational technologies and support for a

clearing center to assist schools and vendors find appropriate best practices for their needs.

To conclude, I believe that HB 607 and these additional steps would build a set of strong and effective privacy protections for Maryland’s student information. Without such strong and effective privacy protection measures, data-driven educational policies and individualized instruction will not be able to succeed.

Biographical Information

Joel R. Reidenberg is the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton University (2013/14) and holds the Stanley D. and Nikki Waxberg Chair in Law at Fordham University where he directs the Center on Law and Information Policy. Reidenberg publishes regularly on both information privacy and information technology law and policy. He has served as an expert adviser to the U.S. Congress, the Federal Trade Commission and the European Commission. Reidenberg is a graduate of Dartmouth College, earned his law degree at Columbia University 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.