Prepared Statement of

Mark MacCarthy
Vice President, Public Policy
Software & Information Industry Association

Before the

Subcommittee on
Early Childhood, Elementary, and Secondary Education

Of the
Committee on Education and the Workforce

And the

Subcommittee on
Cybersecurity, Infrastructure Protection, and Security Technologies

Of the
Committee on Homeland Security

United States House of Representatives

On

"How Data Mining Threatens Student Privacy"

June 25, 2014

On behalf of the Software & Information Industry Association (SIIA) and our member high-tech companies, thank you for inviting me to testify today. I am Mark MacCarthy, SIIA's vice president of public policy. SIIA commends Chairman Meehan and Rokita, Ranking Members Clarke and Loebsack and your respective Committees for holding this hearing to examine student privacy in the digital age.

SIIA is the principal trade association for the software and digital content industry. Many of SIIA's 800 member high-tech companies partner with schools and universities across the country to develop and deliver learning software applications, digital content, web services and related technologies and services that meet teaching, learning and enterprise management needs. All SIIA members depend on the nation's schools for a skilled, high-tech workforce.

Modern information technologies play an increasingly essential role in our education system. SIIA agrees that the effective use of student information to improve learning is concomitant with the obligation to safeguard student data privacy and security. This will require a continued and enhanced trust framework between the triad of stakeholders – parents and schools; schools and service providers; and service providers and parents.

My testimony today will address three questions:

- What are some of the ways students, teachers and schools use technology and leverage data to improve education?
- What are the current policies and evolving practices protecting student privacy and data security?
- Is there a need for new Federal student privacy legislation?

I. Use of Technology and Student Information in Schools

As we move from an industrial-age era model to a customized education model, technology is increasingly mission-critical to making certain all students receive a world-class education, and our nation competes in the global economy. International assessment results and high-tech job openings demonstrate the challenge of ensuring students are college and career ready, including with the STEM (science, technology, engineering and math) and other 21st century skills needed to succeed in this knowledge-based economy.

From adaptive learning software to class scheduling applications to online learning, technologies are enhancing student access and opportunity and enabling administrative operations. Many of these technologies are based on the effective use of student information for educational purposes. As such, technology and data systems are increasingly essential to supporting students, families and educators – providing operational efficiencies, informing practice, and personalizing student learning.

Some of the ways the use of educational technology and student information can enable school operations and improve student learning include:

1. Help Meet the Needs of All Students. Technology enables multiple approaches to learning to effectively address each student's individual learning style, abilities, pace and interests. Through embedded assessment and adaptive content, today's data powered courseware helps teachers deliver lessons and content in the modality, complexity and representation to meet every student's unique needs, rather than teaching to the mean. Predictive analytics can also identify students at risk of dropping out of school. Timely identification enables schools to intervene early in the process.

2. Facilitate Communication and Collaboration. Participation in a variety of controlled virtual and learning communities with peers and experts inspires students and teachers to discover, explore, guide and collaborate. Parents can access information and curriculum, and communicate with teachers in more convenient and powerful ways to support their children's learning.

3. Manage the Education Enterprise. Like businesses, schools are harnessing technology to manage core organizational tasks from accounting to human resources to scheduling. Through data management and analysis tools, administrators can identify performance gaps and effective practices, thus enabling more informed decisions to operate the school more efficiently and effectively.

The recent Obama White House report on data and privacy highlights two complementary main benefits of data in education: personalized learning and research to enhance understanding about learning. It reads, in part: "Data from a student's experience . . . can be precisely tracked, opening the door to understanding how students move through a learning trajectory with greater fidelity, and at greater scale . . ." The opportunity is to use this data-driven understanding to customize student instruction and curriculum based on each student's unique needs.

As outlined above, an essential part of the technology-enabled changes to practices in our schools is the collection, use and sharing of student information for educational purposes. Our educational system has long collected and used student data to operate and inform educational practices, and has routinely done so by using third-party service providers.

Today, new technologies like cloud computing are enhancing school capacity in ways not otherwise possible by providing anytime/anywhere data access, enhanced data management functionality, powerful data analytics, and improved security. The scale of cloud computing enables great expertise and investments in security, which includes predicting and identifying against external threats such as hackers or malware and putting in place the most sophisticated data security technologies. In addition, cloud security guards against more traditional threats such as fire or unlocked file cabinets whereby the technology provides a protection not possible through traditional methods. These tools and techniques allow educators to manage more data in more cost effective, secure and sophisticated ways to inform instruction and enhance school productivity.

We can think of these cloud data systems like a safety deposit box – your valuables are in a bank, but only you have the key and decide who gets access. For many data systems, the provider houses the data and provides data tools, but access is controlled by education administrators with the digital key.

The result of advanced data management and analysis tools is the ability for school systems to better identify students at risk of failure, identify the lessons that best meet each and every student's unique needs, inform decision making, and enhance operations. The goal is to translate data into actionable information so we can be smarter as an educational system about how to meet the needs of each student based on understanding of what is most effective with students like me. We should want our students, families and educators to have all the relevant information, while making sure it is used appropriately for educational purposes and that student data privacy is protected.

II. Current Framework of Student Privacy Practices and Protections

Schools and service providers have a shared responsibility to safeguard the privacy and security of student information. One way they do this is by limiting the collection and uses of student personal information to legitimate educational purposes. They have policies and procedures in place to prevent unauthorized use.

Federal law establishes a framework that restricts the collection and use of student information to what is necessary to accomplish legitimate educational purposes.

The Family Educational Rights and Privacy Act (FERPA) requires that:

- personally identifiable information shared with service providers be limited to uses otherwise performed by the school's own employees,
- the provider be under direct control of the school, and
- the information can only be used for educational purposes.

In addition, the Children's Online Privacy Protection Act (COPPA) requires consent for child-directed online and mobile collectors of personal information from children under the age of 13, both inside and outside of schools, and prohibits the use of information for behavioral advertising. COPPA requires the operator to provide the school with full notice of its collection, use, and disclosure practices.

FERPA and COPPA require parental consent if the school shares personal student information with third parties for non-educational purposes. These laws also require parental consent if the operator wants to use or disclose the information for its own commercial purposes beyond those related to the provision of services to the school.

In addition, the Protection of Pupil Rights Amendment (PPRA) requires parental notice and opportunity to opt-out of activities involving the use of personal information collected from students for marketing and advertising purposes unrelated to the educational purpose for which it was collected.

The U.S. Department of Education has provided some examples of how these rules work in practice to protect student privacy. In its recently released guidance on protecting student privacy while using online educational services, the Department of Education advised that a service provider such as a provider of email service or cafeteria service is not permitted to use student information to target ads to students because this use does not "constitute a legitimate educational interest."

Service providers are also bound by contract and are subject to significant penalties for unauthorized disclosure of personal student information, including a ban on providing services for up to five years. And there's a market incentive: if service providers do not live up to their responsibilities, they will lose the confidence of their customers.

In short, school service providers do not have an independent role in the school system. They cannot just use personal student information as they see fit. School service providers collect personal student information only with the explicit approval of the schools and agencies that they work for. They use this information only for the purpose authorized by those educational institutions.

SIIA recognizes questions and concerns raised by some parents, educators and policy makers. SIIA agrees that the obligation to safeguard student data privacy and security means that continued review and enhancements are needed in the framework of our policies, practices and technologies.

Stakeholders are responding to recent questions and concerns:

- Service providers continuously review and improve data policies, procedures and technologies.
- SIIA has released industry "Best Practices for the Safeguarding of Student Information Privacy and Security for Providers of School Services" that address educational purpose, transparency, school authorization, data security and data breach notification (http://bit.ly/SIIAstudentPrivacyBP).
- The federal government recently updated regulations and guidance for FERPA and COPPA

specific to online educational services.

- The Consortium for School Networking (CoSN), representing school CTOs, recently released a toolkit for protecting Privacy, "Considerations When Choosing an Online Service Provider for your School System."
- School districts are instituting supplemental agreements with their vendors that further specify restrictive data use, security and confidentiality terms.
- School districts and non-profits are developing criteria for the review of apps, websites and cloud-based software, and sharing the criteria and review results.

These policies and agreements enhance a framework of laws and practices that has been highly effective through the years in safeguarding student privacy and data security.

III. The Need for Federal Student Privacy Legislation

SIIA and our member companies agree with the need to review and improve public policies as needed. However, we do not think that new federal legislation is needed at this time. The current legal framework and industry practices adequately protect student privacy. Moreover, new legislation creates substantial risks of harm to the innovative use of information that is essential to improving education for all students and ensuring U.S. economic strength in an increasingly competitive global environment. These risks include:

- New legislative requirements would not provide local communities and school officials with sufficient flexibility, and government actions intended to create a privacy and security floor would instead unintentionally create a digital learning ceiling.
- Policies that are overly restrictive or make impractical requirements would have a chilling effect on schools and service providers that would stifle the emergence of personalized learning environments and the effective use of predictive analytics to improve student learning.

SIIA agrees with the Obama Administration's May 2014 report on data and privacy, which called for "Responsible Educational Innovation in the Digital Age," including that "Students and their families need robust protection against current and emerging harms, but they also deserve access to the learning advancements enabled by technology that promise to empower all students to reach their full potential."

Similarly, the Aspen Institute Task Force on Learning and the Internet's recent report, "Learner at the Center of a Networked World," cautions that "Approaches to providing safety online that are defensive and fear-based are often ineffective and can have the unintended consequence of significantly restricting learning opportunities for young people." SIIA agrees with the Aspen Institute that technology "can be part of the solution by helping create trusted environments."

SIIA recently issued "Policy Guidelines for Building a Student Privacy Trust Framework" (http://bit.ly/SIIAStudentPrivacyPolicyGuidelines) that I ask be included in the record of the hearing.

Finally, while this hearing is focused on student data privacy, I would be remiss without encouraging the Committees to provide additional leadership, regulatory innovation, and investment needed to support the nation's educational system in updating its teacher skills, infrastructure and practices for the digital age.

I would be happy to answer any questions you might have.