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 Schneiderman, SIIA’s senior director of education policy. SIIA commends Assembly Members Buchanan and Chau and your respective committees for holding this hearing to examine student privacy in the digital age and related California policies.

SIIA is the principal trade association for the software and digital content industry. Many of SIIA’s 800 member high-tech companies are based in California. Many partner with schools and universities in California and nationwide 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. As policymakers consider the need for additional legislation and regulation, SIIA wants to ensure policies are appropriately targeted and crafted to ensure there are no unintended or unnecessary barriers to school operations and digital learning opportunities.

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 data privacy and security?
- What are the appropriate policy considerations in California to support the effective use of student data for learning while safeguarding student data privacy and security?
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 delivering a world-class education and ensuring the nation’s competitiveness.

As we move from an industrial-age to a customized education model, technology is increasingly vital 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 nationally and in California 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 mission critical 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.

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.

Yet, SIIA’s Vision K-20 survey found that technology access and use remains relatively modest. In California, 74% of educators report technology as highly important to them, but only 22% report that their institution currently has a high level of technology use.

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 key.

Yet, we are at the early stages of leveraging this information to support teachers and students. California educators responding to SIIA’s Vision survey reported an ideal level of 3.7 (on a 1-4 scale) for the use of information systems that provide digital student and achievement data that support their instructional decisions. However, they report their current level of use at only 2.8.

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.

Education leaders recognize this responsibility. In fact, SIIA’s Vision survey has continually identified the use of security tools to protect student data and privacy as among the top reported use of technology by schools and school agencies. In California, educators report that their current use of such technologies and practices is 3.2 out of a possible 4.0.

The federal 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 federal Children’s Online Privacy Protection Act (COPPA) requires consent for child-directed online and mobile collectors of personal information from children under 13, both inside and outside of schools, and restricts 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 both:
- if the school shares personal student information with third parties for non-educational purposes; and
- 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 federal 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.

Service providers are also bound by contract and are subject to significant penalties for unauthorized disclosure of personal student information. 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.
- 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. Public Policy Considerations for Safeguarding Student Data for Educational Improvement

SIIA and our member companies agree with the need to review and improve public policies as needed. However, we are concerned some of the policy solutions may be ahead of and over-correct the actualized problems.

SIIA provides several broad cautions:

- First, any new legislative requirements must provide local communities and school officials with sufficient flexibility so that government actions intended to create a privacy and security floor do not unintentionally create a digital learning ceiling.
- Second, policies that are overly restrictive or make impractical requirements could have a chilling effect on schools and service providers that stifles the emergence of personalized learning environments.
- Third, any new legislation should be consistent with the substantial protections in existing federal regulations to ensure new laws do not overlap, conflict and confuse.
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.”

SIIA recently issued “Policy Guidelines for Building a Student Privacy Trust Framework” (http://bit.ly/SIIAstudentPrivacyPG). I provided the Committees with the full set of those guidelines and will touch on a few here.

1. **Definition of Student Information**

New policies should limit the scope to student personally identifiable information as defined under federal law. School districts and their service providers use de-identified, aggregate, and other anonymous information for many purposes critical to the delivery and improvement of educational services. New privacy policies should not regulate use of this non-identifiable information. To the extent policies do regulate non-PII, they must ensure that restrictions and requirements are adjusted according to the type of data, and therefore its sensitivity and appropriate uses.

2. **Data Governance, Transparency and Training**

As both technologies and educational practices evolve, schools and families need support to take advantage of the opportunities, as well as to understand and address their responsibilities. The best approach is to educate, equip, and empower schools and educators to make informed decisions that safeguard student data and serve student learning.

Public policies should first and foremost focus on the following:

- **Encourage Transparency by Agencies, Institutions and Service Providers** – SIIA’s best practices include: “Transparency: School service providers disclose in contracts and/or privacy policies what types of student PII are collected directly from students, and for what purposes this information is used or shared with third parties.” Transparency about service provider policies and practices empowers school and agency officials, and parents, with the information they needed to make informed decisions.

- **Ensure Appropriate Data Governance within Public Educational Agencies** – Governance policies put in place state and district level governance bodies – composed of community members, officials, experts and other stakeholders – with responsibility for determining specific student data policies and practices.

- **Build School Technology and Human Capacity for Managing Student Data Privacy and Security** – These supports include professional development for teachers and administrators to be good stewards of personal student information, as well as the technology tools for managing and securing that data. This also includes student digital literacy.

Transparency, governance and capacity empower stakeholders and are alternatives, or at least complements, to policy prohibitions that may not account for unique local and evolving circumstances.

3. **Purposes for the Use and Sharing of Student Information**

SIIA agrees student personal information should not be used for non-educational purposes such as selling data to insurance companies or targeting insurance advertising. SIIA agrees that personal student information
should be used only for the educational purposes for which it was entrusted. The challenge is translating these principles into statute in a manner future-proofed for the wave of digital learning transformation at home and at school.

SIIA’s Student Privacy Best Practices include:
- “Educational Purpose: School service providers collect, use, or share student PII only for educational and related purposes for which they were engaged or directed by the educational institution, in accordance with applicable state and federal laws;” and
- “Authorization: School service providers collect, use, or share student PII only in accordance with the provisions of their privacy policies and contracts with the educational institutions they serve, or with the consent of students or parents as authorized by law, or as otherwise directed by the educational institution or required by law.”

New policies should be formed after consideration of the following:

- School’s Need Flexibility to Operate – In general, educational institutions and agencies must have the flexibility to determine which data to collect, with whom to share it, and for what purposes to best accomplish their operational and educational objectives. One-size-fits-all regulations may not work given the diversity of school sizes, staffing, practices and evolving uses of innovative technologies.

- Privacy Restrictions Should not Conflate “Commercial” with Appropriate Educational Uses – Any restrictions on “commercial” uses of information should be defined so as to not unintentionally prohibit any and all activities simply because the operator is a commercial (e.g., for-profit) entity. Privacy restrictions should not inhibit service providers from using student information for educational uses authorized by the district, such as: for providing the service including through subcontractors and partners; for product evaluation, improvement, and development; and to enable adaptive and customized learning. Among the benefits of digital learning is the ability to make ongoing improvements based on the user experience.

- Encourage Use of Student Information for Educational Purposes – Rather than restricting what should not happen, public policies should encourage sound use of student information to support student learning and school operations. Public policy should enable new models that expose students, teachers, and schools to learning opportunities that “work with students like you.” Parents are seeking information to match apps used at home with their child’s specific needs. So long as PII is not shared with unapproved entities, restrictions around “marketing” or “advertising” for non-educational purposes should not be confused with recommendations about the next appropriate module. In other words, prohibitions should not restrict the providing of information to the student or school about or related to the service they are already using. At the least, these should be local or parent determinations.

- FERPA Authorized Uses of Information Should be Supported – Appropriate uses and disclosure of student PII under new policies should reinforce, or at least not contradict, those allowed under FERPA. These include outsourcing school functions as authorized/directed by the educational institution, research studies, audits and evaluations, public or student safety, student transfer to another school, application or matriculation to an institution of higher education, or as otherwise authorized by parental consent.

4. Deletion of Student Data
SIIA agrees with the general practice that personally identifiable student data should be deleted when no longer needed for the purpose for which it was collected. However, one-size-fits-all state mandatory deletion requirements are impractical due to the variance in data types and uses, as well as in governance.

- Deletion policies must recognize personal student information is often under the direct control of the school and not the service provider, such that service providers often do not have access or authorization to delete that information. In most other cases, service provider use – including deletion – of personally identifiable student information is determined and directed by school requirements.

- Deletion policies must differentiate between types and uses of student information. Privacy deletion requirements should only address personally identifiable information, which is of primary interest with regard to a student’s privacy. Absolute data deletion requirements for aggregated, de-identified and other anonymous data that do not pose a concern for a student’s privacy will jeopardize the important and necessary use of this information for ongoing educational purposes. These include the use of non-identifiable information as the fuel for adaptive software, learning analytics and other algorithmic engines whose benefit is that they get ‘smarter’ based on a continuing flow of usage data. Personal student information may also be needed on an ongoing basis such as for district and state longitudinal accountability systems as well as future transcript and degree verification requests.

- Deletion requirements may also not be appropriate for family-owned student personal accounts, even if perhaps created initially for school purposes. In this model, the intent may be for the student information to travel with the student outside and beyond their school, such as documents they created or information about their performance on a mathematics tutorial app.

5. Contract Requirements

Contract requirements in state law must allow for flexibility between local schools and their service providers. Policies that dictate contract terms must be careful to not impose one-size-fits-all requirements where circumstances and needs may vary. Any state requirements should provide a template identifying what issues should be addressed rather than prescribing the specific terms so as to allow for varied and evolving local circumstances and needs.

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

In conclusion, SIIA agrees with the need to safeguard student data privacy and security. Further policy protections must be carefully crafted so that privacy protection floors do not inadvertently and unnecessarily lead to educational ceilings. SIIA instead encourages new policies to be focused on transparency, governance and capacity to empower parents and school officials to make sound and safe use of student information that advance student learning.

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

Software & Information Industry Association
1090 Vermont Avenue, NW, 6th Floor
Washington, DC 20005