Written Testimony of

Brendan Desetti
Director of Education Policy
Software & Information Industry Association

Submitted to:
Education Committee
Connecticut General Assembly

RE: HB 5469, An Act Concerning Student Data Privacy

March 2, 2016

Chairman Fleischmann, Chairwoman Slossberg, and members of the Education Committee, my name is Brendan Desetti. On behalf of the Software & Information Industry Association (SIIA) and our member high tech companies, I submit our views regarding Raised Bill 5469, An Act Concerning Student Data Privacy.

Technology and data are increasingly important to instruction, school operations and student success. SIIA recognizes the importance of safeguarding student privacy. A strong network of laws, contracts, and business practices now does so. SIIA helped develop the Student Privacy Pledge, now signed by over 240 school service providers clarifying their commitments to the appropriate use of student data to meet legal responsibilities and community expectations.

SIIA appreciates the legislature's review of regulations regarding the use and security of sensitive student information. SIIA is concerned that HB 5469 in its current form will create barriers to the appropriate use of technology and data by Connecticut educators and students, institutions and families, and SIIA calls on the Committee to amend the bill to address these concerns.

As background, SIIA is the principal trade association for the software and digital content industry, representing more than 700 high tech companies. Some 200 SIIA members work with schools in Connecticut and nationwide to develop and deliver school software applications, digital instructional content, online learning services and related technologies. Many of these services involve the use of student information. They are helping to support teachers and instruction, improve student learning, carry out various administrative operations, and improve school productivity and educational performance.

Educational Benefits of Technology & Data

The use of student information in schools is nothing new. From class scheduling to teacher electronic gradebooks to adaptive learning software, our schools have a long history of effectively using student information, and of relying on technologies from school service providers.

Today, newer technologies like hosted (or 'cloud') computing and data analytics are enhancing school capacity, increasing teacher access, improving security, and improving functionality. The result of these

tools is the ability for school systems to better identify students at risk of failure, to better identify the lessons that best meet each student's unique needs, and to more efficiently carry out core school administration. These tools and techniques allow educators to manage more data in more cost effective and sophisticated ways to inform instruction and enhance school productivity

As such, technology and data systems are increasingly mission critical to supporting students, families and educators – providing operational efficiencies, informing practice, and helping address the unique learning needs of each student. Modernizing our educational system through technology is critical to delivering a world-class education to all Connecticut students, and ensuring the international competiveness of the state and the nation.

Student Privacy & Security Protections

Schools and service providers have a strong framework of policies and procedures in place to safeguard the privacy and security of student information. One way they do this is by limiting the use of student personal information to the intended educational purposes.

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

- student personally identifiable information shared with service providers be limited to uses otherwise performed by the school's own employees,
- the provider and information be under direct control of the school, and
- the information can only be used for the intended 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, including related to behavioral advertising, from children under 13, both inside and outside of schools. The school may provide consent only where the collection is for the use and benefit of the school and not for other commercial purposes, and the operator must provide the school with full notice of its collection, use, and disclosure practices.

COPPA and FERPA require parental consent both:

- if the school wants to share personal student information for non-educational purposes; and
- if the operator wants to use or disclose the information for its own commercial purposes.

The Protection of Pupil Rights Amendment (PPRA) prohibits 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, privacy policies and their terms of service agreements, and they are subject to significant penalties for unauthorized disclosure of personal student information. And 241 companies have already signed the Student Privacy Pledge that took effect in January 2015 as an additional, legally enforceable set of a dozen commitments that complements this existing protection framework and clarifies the appropriate use of student data to meet legal responsibilities and community expectations.

There is also a market incentive for service providers: if they do not live up to their responsibilities, they will lose the confidence of their customers.

HB 5469

As Connecticut considers adopting its own student privacy legislation, it is critical to take into account the Federal laws already in place and the many state laws recently enacted around the country. Creating conflicting requirements or restrictions risks limiting student and teacher access to technology and the opportunities it can provide. The following is a partial list of SIIA concerns and suggestions aimed at ensuring HB 5469 supports student privacy without inappropriately limiting student, educator and family technology and data use:

- **Parent Review and Correction:**
  Students and parents should have the right to review their educational record and request correction of inaccurate information. Often times however a service provider does not have a relationship with individual users making it impossible for the provider to verify the authority of an individual seeking a correction or the authenticity of the correction itself. For example, a parent should not be able to request a correction of assessment scores or other grades without the permission of the school district. Provisions providing the right to correction should be clear that a parent or student seeking correction must work through the school, with whom the service provider has a relationship, in order to verify identity and authority to make appropriate corrections.

- **Protecting Security:**
  SIIA is concerned that listing the actions a service provider will take to protect the security and confidentiality of student records will in itself nullify or severely compromise those security measures. Contracts with a government agency, including an education agency, are readily attainable by the public through a Freedom of Information Act request which could allow bad actors to obtain information about security procedures in an effort to thwart them. While service providers can and should be expected to maintain security measures designed to protect the information they hold, they should not be required to disclose information publicly that would compromise those measures.

- **Unauthorized Access and Notification:**
  The bill requires notification within 48 hours of a service provider becoming aware of actual or suspected "unauthorized access" of a student record. SIIA is concerned that this requirement may not recognize the difference in harmful and accidental unauthorized access, such as when a teacher accesses the student record of the wrong student. Over notification can result in "breach fatigue" where parents begin to ignore the flurry of notices and miss one of potential importance. Additionally, the timeframe to initiate notifications is unrealistic. For example, 48 hours does not account for instances in which an increased security risk exists from notification prior to implementing a fix or during an investigation by law enforcement who requests notification not be made immediately.

- **Data Minimization:**
  The bill requires service providers to certify that they will not retain a pupil's records after the pupil is no longer enrolled in the local educational agency. SIIA is concerned that this requirement may not recognize the variance in situations and governance of certain student information. In general, this information, and decisions regarding deletion, are controlled by the school entering into agreement with the provider. For example, a student record may be needed on an ongoing basis such as for district and state longitudinal accountability systems as well as future transcript and degree verification requests from employers and postsecondary institutions.

SIIA is also concerned, in section two, that the bill's deletion requirement does not distinguish between identifiable and non-identifiable information (e.g., de-identified, aggregate, and meta-data). Retention of the latter may be needed in some cases for ongoing operations of the software. Similarly, as is standard regulatory and industry practice, the bill makes no allowances for the de-identification of data as an appropriate alternative to deletion.

- **Commercial or Advertising Purposes**
  The first section of this bill prohibits service providers from using information in individual student records for advertising purposes. These terms are not defined in this section however, and SIIA is concerned that the section could be interpreted to prohibit appropriate and necessary educational activities, such as the ability of providers to support the customization of learning to meet a student's unique needs including through recommendation engines. SIIA also notes that the bill does not distinguish between school purposes and non-educational purposes, which may block student/family access to personalized learning and instructional recommendation engines. For example, the restriction may unduly prohibit a simple notification or recommendation of the next module appropriate for that student, even one provided at no additional cost to the school or student. In that way, the restriction could be interpreted to not allow providing information to the student about or related to the service they are already using.

  In section two, SIIA is concerned that the broad definition of 'Targeted Advertising' could be interpreted to restrict access to services already accessible by students which do not collect, retain, or use student information for advertising purposes but may include advertisements based on the context of the site or service or after a request for information or feedback from the student.

- **School Purpose Definition:**
  SIIA is concerned that even the best designed definition may inadvertently leave out appropriate educational activities. In general, school service providers operate at the direction of the school, but the bill instead relies on a more general standard of activities that "customarily take place at the direction of a teacher or a local or regional board..." Relying on customary practices reduces the ability to institute new practices or develop innovations in education. At one time, lunch cards, barcode scanners, and even computers themselves were not customarily used in education. Now they're indispensable.

- **Operator Disclosure:**
  The bill restricts service providers from disclosing student information with certain exceptions, which include disclosure to a third-party (i.e., a subcontractor) provided that party adheres to certain requirements. However, the bill then strictly prohibits that service provider from further disclosing covered information. SIIA is concerned that this prohibition does not take into account instances in which additional disclosure is necessary to provide the educational service, such as an operator disclosing information to a tutoring service who then discloses information to an individual tutor. A service provider's subcontractor should be permitted to further disclose the information to their subcontractors as necessary to serve the educational purpose, provided they adhere to the same requirements and restrictions.

- **Parental Consent Exemption:**
  The bill clarifies the limitations of service provider use of student covered information to school purposes as defined. However, there may be cases where the student or their family may want the information used for additional purposes. For example, they may want the information shared with a tutor, college, or a scholarship fund or to receive information about other appropriate

educational apps and learning modules. Parents should be allowed to request or provide affirmative consent for additional specific uses of their student's data beyond the contracted educational purpose in response to clear and conspicuous notice.

- **De-Identified and Aggregate Information:**
  The bill seeks to allow an operator to use information other than covered information for certain purposes around product development, evaluation and improvement. Among the great benefits of technology is the ability for operators to monitor use and carry out ongoing review and improvement based on the user experience. SIIA calls for a clarification that service providers may use both de-identified and aggregated student information for R&D purposes. This non-identifiable information is used in R&D to ensure that providers can best serve their users with the most effective educational services.

Thank you for your consideration of these views. I would be pleased to work with you further to ensure any legislation supports safeguarding of student data without creating barriers to important use of technology and data by educators, students and families. Please feel free to contact me at bdesetti@siia.net or (202) 789-4448.

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