June 18, 2018

New York State Education Building
89 Washington Avenue
Albany, NY 12234

Re: Student Data Privacy Public Forum Written Comments

To Whom It May Concern:

On behalf of the Software & Information Industry Association, I submit the following comments for the New York State Education Department to consider as it develops regulations implementing New York’s student data privacy law (“2-d”) and contemplates possible additions to Education Law 2-d bill of rights for data security and privacy.

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 New York 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.

Technology and data are increasingly important to instruction, school operations and student success. Student privacy and security are mandatory factors when implementing any technology or data strategy in the classroom. SIIA has worked collaboratively with states and stakeholders over the past several years to find ways to protect the privacy of students across the United States.

General Comments on Student Data Privacy

Educational technology providers agree it is necessary to safeguard student privacy: they take their compliance responsibilities seriously and work hard to maintain the trust of their users. Federal and state activities on student data privacy dramatically increased since the passage of 2-d. Over 100 laws have been passed across the country related to student data privacy. The U.S. Department of Education has released several guidance documents related to student privacy and educational technology. There are several student data privacy bills up for consideration in the U.S. Congress.

Additionally, in late 2014, SIIA and the Future of Privacy Forum (“FPF”) launched the Student Privacy Pledge (“pledge”). The pledge is built on public commitments regarding the collection, maintenance, and use of student personal information that meet and exceed the federal requirements for student data privacy. There are currently 344 signatories of the pledge.

On June 13, 2016, SIIA and other organizations submitted a letter to the New York State Senate on a bill related to student data privacy under consideration. In that letter, we wrote, “We recommend that any new student privacy legislation work to align New York State law with the similar privacy requirements passed in other states around the nation.” We echo that statement today and urge the New York Education Department to issue regulations that offer strong student privacy protections, align with
other states across the country, and allow for continued access to innovative educational tools and service provider. Our preliminary recommendations follow:

- **Personally Identifiable Information**
  The law currently aligns the definition of PII to the federal Family Educational Rights and Privacy Act (FERPA). In the dozens of laws passed since 2014, policymakers have been explicit in defining PII. If policymakers wish to further define PII through regulations, we urge alignment with laws passed in many other states such as California and Texas.¹

- **Security**
  SIIA members large and small prioritize the security of education records. 2-d explicitly requires the use of encryption technology to “protect data while in motion or in its custody from unauthorized disclosure” and requires the use of a technology or methodology aligning those security protections to those required under HIPAA. Some companies may be able to provide greater protections that go above and beyond what is required by HIPAA. SIIA urges policymakers to allow flexibility when protecting student data when companies are able to provide a greater level of security than prescribed by the federal government.

- **Contracting**
  Technology finds the way into the classroom in a number of ways. One of the more common ways is through a simple terms of service agreement or user license. These are often referred to as “click-wrap agreements” where service terms are outlined and a user “clicks” to accept them. These terms are often carefully written to meet federal and state legal requirements especially when it comes to education technology. 2-d defines a “third-party contractor” as any person or entity that receives student data from an educational agency “pursuant to a contract or other written agreement.” We urge policymakers to further define a “contract or other written agreement” in a way that would allow for the use of terms of service agreements or other “click-wrap” type agreements so long as those terms meet the requirements of 2-d.

**Suggestions for 2-d Bill of Rights for Data Privacy and Security**

A parent’s bill of rights for data privacy and security should take steps to outline the methods in which

---

¹ Texas’s recently passed student privacy law defines personally identifiable information as the following, “(1) "Covered information" means personally identifiable information or information that is linked to personally identifiable information, in any media or format, that is not publicly available and is:

(A) created by or provided to an operator by a student or the student’s parent in the course of the student’s or parent’s use of the operator’s website, online service, online application, or mobile application for a school purpose;

(B) created by or provided to an operator by an employee of a school district or school campus for a school purpose; or

(C) gathered by an operator through the operation of the operator's website, online service, online application, or mobile application for a school purpose and personally identifies a student, including the student’s educational record, electronic mail, first and last name, home address, telephone number, electronic mail address, information that allows physical or online contact, discipline records, test results, special education data, juvenile delinquency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, student identifiers, search activity, photograph, voice recordings, or geolocation information.”
students and parents can exercise their right to review their educational record and request correction of inaccurate information. The school should facilitate parent and student access and review, as required by the Family Educational Rights and Privacy Act (FERPA). 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 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. Access and amendment rights provisions 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.

Conclusion

Thank you for time and consideration of all stakeholder views as you take additional steps to protect student privacy in New York. Please feel free to contact me at skloek@siia.net or (202) 789-4448.

Sincerely,

Sara Kloek
Director of Education Policy
Software & Information Industry Association