3/29/2019

Temitope Akinyemi
NYS Education Department
Office of Higher Education
89 Washington Avenue, Room 975 EBA
Albany, NY 12234

Dear Ms. Akinyemi,

On behalf of the Software & Information Industry Association, we submit the following comments in response to the New York State Education Department’s proposed regulatory changes to “safeguard the Personally Identifiable information of students and certain school personnel.” We worked with policymakers in New York prior to the passage of the student privacy law in 2014 and look forward to working with policymakers once again as this process moves forward.

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. SIIA members 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.

Current Status of 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. States across the United States have passed over 100 laws on student data privacy since the passage of Education Law Section 2-d (“2-d”). Federally, the U.S. Department of Education has released several guidance documents related to student privacy and educational technology. There are several privacy bills up for consideration in the U.S. Congress.

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 350 signatories of the pledge.

We’re pleased that the regulations include click-wrap agreements in the definition of “Contract or other written agreement” and urge the NYSED to keep the definition, as written, in the proposed regulations. This reflects current practices and aligns with other student data privacy laws across the country.

We identified some areas where we would request a review and update to reflect current best practices and align with existing New York law. These areas include:

1. The definition of commercial or marketing purpose;
2. Service providers and contractors;
3. The multiple security standards outlined in the regulations;
4. Civil penalties;
5. The lack of industry representation on the Data Privacy Advisory Council.

**Scope of Commercial and Marketing Purpose**

2-d specifically states that “a student’s personally identifiable information cannot be sold or released for any commercial purposes.” The law also says that “personally identifiable information maintained by educational agencies, including data provided to third party contractors and their assignees, shall not be sold or used for marketing purposes.” The proposed regulations expand the scope of both of these provisions by defining “commercial or marketing purpose means the sale of student data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve, or market products or services to students.” We believe these regulations go beyond the scope and intention of the law and could cause some unintended consequences if left as written.

Restrictions on the use of student data are common across state and federal student data privacy laws. FERPA, for example, requires that “personally identifiable information from education records may be used only for the purposes for which the disclosure was made.” The Children’s Online Privacy Protection Act (COPPA) allows a school to consent to the release of a student’s data to a company that is subject to COPPA but that consent is “limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.” The FTC’s COPPA Frequently Asked Questions outline that a commercial purpose would include a third party contractor using students’ personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the third party contractor. The Student Online Personal Information Protection Act (SOPIPA), first

---

1 § 99.31(a)(1)(i)(B)
2 [https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools)
passed in California and later passed in a number of other states across the country, include provisions that ban the use of student information to engage in targeted advertising, use information to amass a profile, and from disclosing covered information, with some exceptions including for legal compliance, judicial process, and for the safety of users or security of the site.

While the proposed regulatory language intends to protect student personally identifiable information, it fails to consider how student data is used by educational technology companies. The specific provisions that prohibit the use of student data to “develop” or “improve” products “whether directly or indirectly” may prevent companies from using student data to identify whether or not a particular feature of their educational program is improving student outcomes and then to later improve the product to improve student outcomes. If a third party contractor has properly de-identified the data it collected in accordance with the requirements of FERPA (34 CFR 99.31(b), it should be able to use that data to improve or create new educational products and services that the operator could market to schools and districts. The contractor should also be able to use deidentified data to demonstrate product efficacy.

The proposed regulatory language definition of commercial or marketing purpose expands on the 2-d definition of commercial purpose and could be read in a way that effectively bans any school from working with a for-profit entity. Businesses making education technology products, by the nature of being a business, do profit from the sales of their products. That language should be stricken from the regulations.

The provisions also exclude promotion of colleges, scholarships, tutoring services, educational materials and related resources to students who are deserving or in need. With prior consent from the parent or legal guardian, and so long as the materials are there to support an educational purpose, promotion of educational services should be allowed.

SIIA Recommendation: Review and revise the definition of “Commercial or Marketing Purpose” to state “use or disclosure of student data for a purpose other than that permitted in Education Law Section 2-d and for which it was disclosed. This includes the selling the information to a third party, and targeting individual students with directed advertisements, except, with the prior consent of the parent or legal guardian, to the extent that such directed materials are for products and services that support an educational purpose or goal. This prohibition does not apply to the purchase, merger, or other type of acquisition of a third party contractor by another entity, provided that the successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.”

Service Providers and Contractors

2-d requires third party contractors to provide information on “how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and
security requirements.” The proposed regulations intend to require that subcontractors to third party providers adhere to the same standards as the third party providers. We agree that subcontractors should be required to protect the data according to the contract signed by the third party provider. The proposed language, as written, is a bit unclear. We request that the NYSED review and revise accordingly.

SIIA Recommendation: Review and revise the subcontractor obligations as follows, “an assurance that the third party contractor will (a) prohibit the subcontractor from using student data or teacher or principal data for any purpose other than providing the contracted service to, or on behalf of, the third party contractor, (b) prohibits the subcontractor from disclosing student data or teacher or principal data provided by the third party contractor to subsequent third parties, and (c) requires the subcontractor to comply with subsection 1.1 of this section.”

Consistency of Security Standards

When New York passed 2-d, policymakers included a specific requirement for third party contractors to use encryption technology to protect data using a technology or methodology outlined in Section 13402(H)(2) of Public Law 111-5 (HIPAA encryption standard). The HIPAA encryption standard is designed to protect the privacy of personal health information that is created, received, used, or maintained by a covered entity. The rule is written for entities that are well-versed in a vocabulary that does not necessarily align with the vocabulary used in the education sector.

The proposed regulations refer to two different security standards – the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST CSF) and the HIPAA encryption standard. While there is some alignment between the standards, they do have different requirements. The regulations adopt NIST CSF for educational agencies but requires third party contractors, under both the law and the proposed regulations, to follow HIPAA’s encryption standard to protect data in motion or in its custody. These separate requirements may cause confusion for school staff or third party contractors as they evaluate and purchase products for use in the classroom.

SIIA recommendation: The NYSED should provide technical assistance on the two security standards to educational entities.

Fault-Based Civil Penalties

Section 121.11 is written in a way that may allow the Commissioner to issue civil penalties to a third party contractor even if a data breach is done without intent knowledge, recklessness, or gross negligence. It should be rewritten to state that penalties may only be imposed if they find that a third party has breached or violated the duties listed, with the intention of so doing, or due to recklessness or gross negligence.
SIIA recommendation: Section 121.11 should be rewritten to state that penalties may only be imposed if the third party has breached or violated the duties listed, with the intention of so doing, or due to recklessness or gross negligence. This could read, “If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Commissioner shall determine that no penalty be issued upon the third party contractor.”

Stakeholder Involvement in the Data Privacy Advisory Committee

In 2017, the NYSED’s Chief Privacy Officer created the Data Privacy Advisory Council (DPAC) charged “with assisting in the development of regulatory language and recommending a standard for educational agency data security and privacy policies and practices.” The NYSED’s January 14, 2019 press release notes that the DPAC “consists of members drawn from diverse stakeholder groups and includes parents, industry advocates, administrative and teacher organizations and information technology experts.” A review of the membership of the DPAC shows no industry advocates from the third party providers the law intends to regulate. The inclusion of third party providers throughout the process would inform the process with crucial field information on current use and practice as well as greatly reduce the chance of unintended consequences to result in robust, balanced regulations.

SIIA Recommendation: We encourage the NYSED to include all stakeholders, including parties that will be regulated by a law, throughout the process.

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 for any additional information.

Respectfully submitted,

Sara Kloek
Director of Education Policy
Software & Information Industry Association