The Honorable Xavier Becerra  
Attorney General, State of California  
1300 I Street  
Sacramento, CA 95814

Via Email to: Eleanor Blume (Eleanor.blume@doj.ca.gov) and privacyregulations@doj.ca.gov

Dear Attorney General Becerra,

On behalf of the Software and Information Industry Association (SIIA), I write in regard to the conflicts between the Family Educational Rights and Privacy Act (FERPA), the Student Online Personal Information Protection Act (SOPIPA), section 49073.1 of California’s Education Code (AB 1584), and the California Consumer Privacy Act (CCPA). Nearly 200 of our members are working with schools in California to develop and deliver software applications, digital instructional content, online learning services, and related technologies. Many of these technologies use student information to help educators improve student outcomes.

Our members serve schools in a number of ways. Some provide online curriculum, some provide administrative tools such as cloud-based grade books and student information systems, and others provide hardware that help students connect to a diverse collection of educational materials.

SIIA appreciates the work California legislators, regulators, schools, and companies have done to protect student privacy and request clarification on the intersection of these laws. We are writing because the recently enacted CCPA creates conflicts with existing student privacy laws in ways that the legislature could not possibly have intended. This letter is intended to identify the conflicts between the CCPA and existing law, and to propose language that resolves potential confusion.

Student Privacy is Regulated by California Law and Federal Statutes

California, starting with student privacy legislation in 2014 and, more recently, comprehensive consumer privacy legislation, has been a leader in privacy. Unfortunately, the CCPA has created conflicts with existing student privacy legislation resulting in a lack of clarity for schools, parents, and education technology companies. (This letter will use “edtech companies” or “edtech” throughout instead of using the terms used in the specific laws such as third parties, online educational services, businesses, and operators.) When working at the direction of schools – public and private; K-12 and post-secondary – our companies are under strict and overlapping legal obligations to protect student privacy.

First, the federal Family Educational Rights and Privacy Act (FERPA), restricts how schools may share student education records and student personally identifiable information as a condition of receiving
FERPA therefore governs most public K-12 schools, some private K-12 schools, and most public and private institutions of higher education. Substantively, FERPA generally requires affirmative parental consent before any release of a student’s personal information, and provides parents with the right to inspect educational records, and challenge inaccuracies in those records in appropriate circumstances.

Narrow exceptions to the consent requirement exist that enable key educational functions. For example, FERPA’s “school official exception” allows schools to outsource institutional services or functions to contractors (e.g., bus drivers), volunteers, or other third parties but only if those actors perform a function that would otherwise be done by school employees. In addition, the school must directly control such an actor’s use and maintenance of education records, and the school is responsible to ensure that such an actor only uses personally identifiable information for narrow and school-related purposes for which the information was disclosed. Finally, if the school is using the school official exception to disclose information without consent, it must tell parents about the fact that the school is using the exception. Consequences for both an ed tech company and the school of any privacy violation are severe: If a vendor violates the non-disclosure requirements of FERPA, the school cannot provide access to personal information for at least five years.

California has enacted two separate statutes that supplement FERPA’s protection. First, AB 1584 enhances FERPA’s protection by requiring schools (or “local educational agencies,” in the parlance of the statute) to include privacy-protective provisions in their agreements with ed tech companies. More specifically, AB 1584 mandates that contracts between schools and edtech companies bar edtech companies from using student records for purposes other than those permitted by that contract. Among other things, the contract must include a “certification that a pupil’s records shall not be retained or available upon completion of the terms of the contract and a description of how that

---

1 20 U.S.C. § 1232g; 34 CFR Part 99
2 See 20 U.S.C. § 1232(g).
3 34 CFR Part 99.31 (a)(1)(i)
4 34 CFR Part 99.31 (a)(1)(ii)
5 20 U.S. Code § 1232g (b) (4) (B). The Department of Education has supplemented FERPA’s statutory and regulatory provisions with guidance on using edtech in the classroom that clarifies best practices on how schools should effectively exercise direct control over the use and maintenance of education records and related PII by ed tech companies. These practices include suggestions for data deletion and destruction, a process to facilitate parental access to the information through the school, and requirements to use personal information only for purposes outlined in the agreement with the school. See https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20February%202014%20_0.pdf; https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf
certification will be enforced” and an explicit prohibition on using student information (“pupil records”) to engage in targeted advertising.  

While AB 1584 and FERPA regulate schools, SOPIPA directly regulates educational technology companies. SOPIPA prohibits edtech (or anyone else) from knowingly engaging in targeted advertising to students or parents, using covered information to amass a profile about a K-12 student, selling student information, or disclosing covered information. It also requires companies to maintain reasonable security procedures and practices, and delete information if requested by a school or district.  

Read together, SOPIPA, AB 1584, and FERPA’s requirements recognize the unique relationship between an edtech company and a school and establish guardrails for the use of student data that are both protective of student privacy and tailored to the educational context. Both AB 1584 and FERPA include provisions that require the school or the contract between a school and a vendor to set procedures for the parent or student to request access to student records. SOPIPA prohibits the sale of covered information, and the creation of profiles. We do not believe that the legislature intended the CCPA to interfere with the operation of these statutes. But unfortunately, that is exactly what the CCPA does.

### The CCPA Creates Conflicting Compliance Obligations and Direct Operational Concerns for Companies Operating in Education.

The CCPA establishes the rights of California residents to access, deletion, and porting of personal data from certain “businesses.” Included in the definition of “personal information” is “education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.” As many edtech companies will meet the definition of “business,” edtech companies have ensuing obligations including transparency, opt-out, and deletion on request.

When they are acting in the educational sector, CCPA places edtech companies in the impossible position of choosing between compliance with two different statutory regimes: one designed specifically for the education sector, and one applicable to consumers generally. For example, FERPA

---

6 Cal. Ed. Code § 49073.1 (b)  
7 Cal. B.&P. Code § 22584 (b).  
8 Cal. B.&P. Code § 22584 (b) (4)(E)  
10 34 CFR 99.10  
11 Cal. Civ. Code § 1798.198(a)  
12 Cal. Civ. Code § 1798.110 (a)  
13 Cal. Civ. Code § 1798.120 (a)  
gives parents and eligible students the right to inspect and amend educational records maintained by
the school. FERPA, does not, however, give parents and eligible students the right to request deletion
of their student’s education record. The CCPA gives consumers the right to request deletion of
personal information from a business. It is not clear, however, how an edtech company that is
maintaining education records under a contract with a school district must respond if a student
contacts the company to request deletion of their information. Should a company uphold the terms of
their contract with a school which conforms to FERPA, AB 1584, and SOPIPA requirements? Or should
the company adhere to the requirements of CCPA and delete the information without the school
knowledge?

Similarly, SOPIPA requires deletion of covered information “if the school or district requests deletion of
data under the control of the school or district.” And AB 1584 expressly provides that contracts with
edtech companies ensure that all pupil records “continue to be the property of and under control of
the local educational agency.” It also mandates that the contracts describe a means for pupils to
retain control of “pupil-generated content,” except for standardized assessments where pupil access
would jeopardize the utility of those tools.

FERPA, SOPIPA, and AB 1548 represent strong and context-specific privacy rules that recognize that in
the educational sector, edtech companies will very often have no direct legal relationship with the
person that the CCPA treats as the “consumer.” Nonetheless, all of this information, as well as the
edtech companies operating in this space, are subject to the CCPA’s obligations. SIIA members are also
concerned about the CCPA’s application to the security of standardized assessment tools—not just in
K-12 educational assessments, but also in higher education, healthcare, professional certification,
government licensure, and academic admission.

We respectfully request that these operational issues for edtech companies and schools are clarified
before the effective date of the CCPA. In the Appendix to this letter, SIIA details a number of proposed
amendments to the law that would address these concerns. We respectfully request a meeting with
you or your staff to discuss these issues. In the interim, please do not hesitate to contact Chris Mohr at
cmohr@siia.net and Sara Kloek at skloek@siia.net if we may be of assistance.

Sincerely,

Ken Wasch
President & CEO
Software & Information Industry Association

17 Id. (d)(4)
APPENDIX: AMENDMENTS

The protections afforded to California residents, such as access and deletion, through the CCPA are already included in the frameworks of federal and state student privacy laws. The amendments that follow are based on the specific operational problems that the CCPA poses in the educational sector:

- Edtech companies act as service providers to the schools and do not have a direct relationship with the student or the parent. The CCPA does not take account of this reality. A company must provide service to a “business” in order to qualify as a service provider under the bill, and schools, not-for-profits, or other governmental entities do not meet the statute’s definition of “business.”

- AB 1584 imposes specific requirements to protect pupil personal information in contracts between a school and an edtech company. An edtech company should not have to choose between violating legally valid contract clauses required by AB 1584 and CCPA compliance.

- The definition of “personal information” could be read to apply to information acquired by edtech companies not just in the kinds of standardized tests used in grade schools, but also in other fields, such as those that use standardized tests for professional certification and testing.

1. Clarify Definition of Service Provider

This amendment would clarify that companies acting on behalf of another entity (such as a government entity) qualify as a service provider so long as their activity consists of providing services under a contract that meets the requirements outlined by the bill. It is also intended to ensure that the service provider does not face liability when it acts as for a business either with respect to deletion, opt-out, or notice so long as it is acting as the instrument of a business. The amendment also deletes redundant language regarding “retaining and using.” That deletion is not intended to change the statute’s effect.

1798.140.

(v) “Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects or processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose another entity, including a for-profit or nonprofit, or federal, state or local governmental entity, pursuant to a written contract with such an entity, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title.
required by law, or specified by such entity, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. A service provider shall not be deemed a “business” under this title to the extent that the collection, processing sale or use of personal information by the service provider is done only: (1) as a service provider for and on behalf of another entity; and (2) for the purposes of performing the services specified in the contract with such entity or otherwise permitted by this title, required by law, or directed by such entity.

2. **Clarify that a business need not breach its contracts to comply with the CCPA**

   This amendment would clarify that companies performing their duties under a written contract qualify for the exemption under 1798.105.

   1798.105

   (d)(8) “legal obligation, including a contractual obligation.”

3. **Clarify that standardized assessments and responses do not need to be disclosed where validity and reliability would be compromised**

   Assessments are critical in assessing learning in the education area, diagnosing medical issues in the health area, and evaluating competency in a number of other areas. Demonstrating competence ensures many public benefits—including health and safety—by proving that individuals who must be licensed or certified to practice a trade or profession in a State have objectively shown they have the necessary knowledge and skills to competently perform their jobs. In other circumstances, such demonstration of competence can be an important consideration in admission to secondary school, college or graduate school, or the satisfaction of academic requirements or meeting the standards for a certification required by employers in any number of fields. Access to a standardized assessment and answers outside of the testing environment can materially affect the integrity of the assessment process. To those for whom they are conducted, as well as for the countless others who rely upon their integrity in many different ways, these tests are matters of consequence. It can cost thousands of dollars to develop a single valid test question and answer. It is vital to not mandate disclosure where the validity and reliability of the assessment would be impaired.

   AB 1584 recognizes this fact by excluding certain assessments from the definition of “pupil-generated content” that would otherwise be required to be given to the student, and the “reliability and validity” language in the suggestion below is drawn from that statute. Compare Cal. Ed. Code 49073.1 (d)(4) (definition of pupil generated content).

   A new 1798.145(g) (renumber subsequent sections accordingly):

   This title does not require a business to disclose a standardized assessment or a consumer’s
specific responses to the assessment where consumer access, possession or control would jeopardize the validity and reliability of that assessment.

4. **Delete 1798.140(o)(1)(J) (educational information in the definition of personal information) and renumber accordingly**

As mentioned above, existing law pervasively regulates the acquisition and use of information in the education space. While this change in and of itself would not undo the conflicts with other laws due to the breadth of the CCPA’s definition of “personal information”, when read against the other changes to the statute it will help clarify the legislature’s intent not to interfere with the ordinary operations of schools.