Date of Hearing: January 13, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1159 (Addis) – As Amended January 5, 2026

## PROPOSED AMENDMENTS

**SUBJECT**: Student personal information

## SYNOPSIS

*Existing law, the K-12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA), establishes privacy protections for students in California's preschools and K-12 public schools. The California Consumer Privacy Act (CCPA) offers additional privacy protections for consumers of all ages when it comes to the personal data collected by large for-profit businesses. However, all these statutes naturally contain gaps and loopholes, especially as technology rapidly advances and the quest for data in the form of personal information about Californians becomes more valuable.*

*This bill, sponsored by Privacy Rights Clearinghouse, is intended to address some of those gaps as they pertain to students. Toward that end, this bill creates the Higher Education Student Information Protection Act (HESIPA), which extends the protections contained in KOPIPA and ELPIPA to higher education students. In addition, among other provisions, the bill increases privacy protections for all students by:*

1. *Prohibiting education technology (EdTech) operators from using student data to train artificial intelligence systems.*

2. *Prohibiting the collection, use, or disclosure of especially sensitive student information (reproductive/sexual health, immigration status, sexual orientation, gender identity) to protect vulnerable students.*

3. *Implementing data minimization requirements and limiting retention to what is "reasonably necessary" for the specific purpose for which the information was collected.*

*As discussed in this analysis evidence supports the need for more rigorous privacy protections for California students. Closing these gaps when it comes to protecting the private information of students and their parents furthers California's privacy goals and protects Californian's fundamental right to determine who should have their personal information.*

*Comment 6 sets forth two minor amendments:*

1. *In HESIPA, the sharing and sale of covered information will not only have to benefit the higher education institution, but it also must benefit the student. Similarly, in KOPIPA and ELPIPA the sharing and sale must benefit the student, parent, or teacher.*

2. *Clarifies in all three sections that operators or their third-party vendors can only use deidentified data to train generative artificial intelligence tools.*

*Due to the tight timelines related to two-year bills, the amendments, if approved by this Committee, will be taken in the Judiciary Committee.*

*The bill is supported by a number of privacy, social justice, labor, and educational groups, including the California Faculty Association, the California Federation of Teachers, Secure Justice, Courage California, and Oakland Privacy.*

*In opposition, the College Board argues that the bill undermines "foundational student activities, such as sending SAT or AP scores to scholarship programs, the ability for adult learners to exercise consent over their own data, and students' ability to receive information tied directly to their in-school assessments." The College Board, ACT Education Corporation, The California Chamber of Commerce, TechNet, and the Computer and Communications Industry Association are in opposition.*

*If passed by this Committee, this bill will next be heard by the Judiciary Committee.*

**EXISTING LAW**:

1) Establishes the Children's Online Privacy Protection Act of 1998, which imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. (15 U.S.C.S. § 6501; 16 C.F.R. Part 312.)

2) Establishes the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. (20 U.S.C. § 1232g; 34 C.F.R. Part 99.)

3) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

4) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

5) Defines "personal information" under the CCPA as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." (Civ. Code § 1798.140(v)(1).)

6) Establishes KOPIPA to restrict the use and disclosure of students' "covered information," which means personally identifiable information or materials, in any media or format that meets the definition. (Bus. & Prof. Code § 22584.)

7) Prohibits, pursuant to KOPIPA, operators from knowingly engaging in targeted advertising, using information about students to create a profile about them except in furtherance of K-12 school purposes, selling students' information, or disclosing their information, except as provided. (Bus. & Prof. Code § 22584(b).)

8) Requires an operator to delete a pupil's CCPA-excluded covered information under the operator's control if a parent, guardian, adult pupil requests the deletion of the information if the pupil has not been enrolled in the school for 60 days or more. (Bus. & Prof. Code § 22584(d)(3).)

9) Defines the following terms for purposes of KOPIPA:

   a) "Covered information" as personally identifiable information or materials, in any media or format that meets any of the following:

      i) It is created or provided by a pupil, or the pupil's parent or legal guardian, to an operator in the course of the pupil's, parents', or legal guardian's use of the operator's site, service, or application for the school's purposes.

      ii) It is created or provided by an employee or agent of the preschool, prekindergarten, school district, local educational agency, or county office of education, to an operator.

      iii) It is gathered by an operator through the operation of a site, service, or application, as defined in number 7, and is descriptive of a pupil or otherwise identifies a pupil, including, but not limited to, information in the pupil's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency 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, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. (Bus. & Prof. Code §§ 22584(i) & 22586(i).)

   b) "Operator" as the operator of a website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.

   c) "K-12 school purposes" as purposes that customarily take place at the direction of the K-12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school. (Bus. & Prof. Code § 22584.)

10) Establishes ELPIPA, which extends the protections of KOPIPA to pupils in preschool and prekindergarten. (Bus. & Prof. Code § 22586.)

11) Prohibits an operator of an Internet Web site, online service, online application, or mobile application, as specified, from marketing specified types of products or services to a minor and from knowingly using, disclosing, compiling, or knowingly allowing a 3rd party to use,

disclose, or compile, the personal information of a minor for the purpose of marketing or advertising specified types of products or services. It also authorizes minor users to remove, or to request and obtain removal of, content or information publicly posted by the minor, subject to specified conditions and exceptions. (Bus. & Prof. Code § 22580.)

12) Defines "artificial intelligence" as an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments. (Civ. Code § 3110(a).)

13) Defines "generative artificial intelligence" as artificial intelligence that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence's training data. (Civ. Code § 3110(c).)

14) Defines "trains a generative artificial intelligence system or service" as including testing, validating, or fine tuning by the developer of the artificial intelligence system or service. (Civ. Code § 3110(c).)

**THIS BILL**:

1) Creates the Higher Education Student Information Protection Act (HESIPA), which extends the protections of the K-12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA) to higher education students.

2) Defines the following terms for the purposes of HESIPA:

    a) "Higher education institution" as a postsecondary institution, vocational program, or postgraduate program that is accredited by an accrediting agency or organization recognized by the state or the United States Department of Education.

    b) "Higher education purposes" as purposes that customarily take place at the direction of the instructor or higher education institution or aid in the administration of higher education institution activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students and higher education institution personnel or are for the use and benefit of the higher education institution.

3) Defines the following in HESIPA, KOPIPA and ELPIPA[1]:

    a) "Artificial intelligence," "Generative artificial intelligence," and "Train a generative artificial intelligence system or service" as having the same definition as in Civil Code section 3110.

    b) "Deidentified" as information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household, if the operator that possesses the information does all the following:

---

[1] All changes subsequently described in the bill summary are included in HESIPA, KOPIPA, and ELPIPA.

i) Takes reasonable measures to ensure that the information cannot be associated with an individual or household.

ii) Publicly commits to maintaining and using the information in a deidentified form and will not attempt to reidentify it.

iii) Contractually obligates any recipient of the information to meet the above criteria.

4) Adds to the definition of "covered information" demographics, extracurricular activities, behavioral information, and device identifiers. For higher education, "covered information" also includes "course of study."

5) Expands the definition of "operator" to include providers of educational software or services, including digital textbooks.

6) Prohibits the sale of a student's information, including covered information, except in specific circumstances, as defined.

7) Prohibits the use of covered information to train a generative artificial intelligence system.

8) Prohibits the collection, use, retention, or disclosure of information relating to a student's reproductive or sexual health, immigration status, sexual orientation, or gender identity.

9) Requires an operator to retain covered information only as long as necessary to fulfill the specific purpose for which the information was collected and delete the information in a manner that protects the collected information.

10) Clarifies that operators are not required to delete mandatory permanent student records.

11) Requires an operator to establish, implement, and maintain a written data retention policy.

12) Prohibits a contractor from retaining information longer than the school or education agency retains the same information.

13) Requires an operator to disclose to a student, or a student's parent or guardian if the student is under 18 years of age, the California Consumer Privacy and Protection Act (CCPA)-excluded covered information, as defined.

14) Allows students or their parents and guardians to bring a civil action against an operator that fails to comply with the required protections, as defined.

**COMMENTS**:

1) **Author's statement**. According to the author:

The Student Online Personal Information Protection Act and the Early Learner Personal Information Protection Act were landmark pieces of legislation that created protections for student and early learner data. However, technological progress has outpaced the legal protections provided by these laws, leaving students and early learners vulnerable to irresponsible collection, usage, and disclosure of their data. Additionally, students in California's institutions of higher education completely lack any sort of robust educational

data protections. AB 1159, the CA Learner Personal Information Protection Act, modernizes existing data protections in the education field and extends those protections to students in higher education, ensuring that all students can learn safely and securely in an increasingly digital world.

2) **Privacy protections for students.** The Family Educational Rights and Privacy Act (FERPA) is the primary law that protects the privacy of student records. It applies to all educational institutions that receive federal funds. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when they reach the age of 18 or attends a school beyond the high school level. Such students are deemed "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

- Parents or eligible students have the right to request that a school correct records that they believe are inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

Under FERPA, schools must generally have written permission from the parent or eligible student in order to release information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to certain parties or under certain conditions.

While FERPA provides certain privacy protections for students and generally prohibits a school from sharing a student's education information without permission, it "did not anticipate the explosion in online learning. Students shed streams of data about their academic progress, work habits, learning styles and personal interests as they navigate educational Websites. All that data has potential commercial value: It could be used to target ads to the kids and their families, or to build profiles on them ..."[2]

California became the national leader on student privacy when it unanimously passed SB 1177 (Steinberg, Ch. 839, Stats. 2014), establishing KOPIPA. KOPIPA was California's response to reports regarding uses of student information and the inadequacies of state and federal law in protecting student personal information. In particular, FERPA applies only to schools, not to third parties who operate educational websites, services, or applications.

---

[2] Stephanie Simon, *The Big Biz of Spying on Little Kids*, Politico, (May 15, 2014.) https://www.politico.com/story/2014/05/data-mining-your-children-106676.

KOPIPA restricts the use and disclosure of the personally identifiable information or materials of K-12 students.[3] It regulates operators of websites, online services, online applications, or mobile applications with actual knowledge that the sites, services, or applications are used primarily for K–12 school purposes and were designed and marketed for K–12 school purposes. It prohibits operators from knowingly engaging in specified activities with respect to their site, service, or application. These activities include:

- Engaging in targeted advertising when the targeting of the advertising is based upon any information that the operator has acquired because of the use of that operator's site, service, or application.

- Use of information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

- Selling a student's information.

KOPIPA also restricts disclosing covered information but provides various exceptions, including where the disclosure is in furtherance of the K–12 purpose of the site, service, or application or to law enforcement. Operators are also required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.

In 2016, the protections in KOPIPA were extended to pre-school and pre-kindergarten students and their parents with the passage of the Early Learning Personal Information Protection Act (ELPIPA) (AB 2799 Chau; Ch. 620, Stats of 2016.)

Since KOPIPA took effect a decade ago, the use of technology in education has accelerated rapidly, in large part due to the COVID-19 pandemic which required schools to shift to remote and online learning seemingly overnight. The use of technology has continued to grow, most recently with the introduction of generative artificial intelligence in classrooms and homes. For example, OpenAI has provided its chatbot, ChatGPT to approximately 500,000 students and almost 65,000 staff and faculty in the California State University system. Similarly, in recent years AI tools, including chat bots, have made their way into K-12 classrooms, with more and more teachers, students, and parents using AI tools as a key component of education despite research studies like a 2025 study from Carnegie Mellon and Microsoft that showed that using GenAI tools may reduce critical thinking skills.[4] According to the California Federation of Teachers writing in support of the bill, students from preschool through university now maintain a near-constant online presence via a profusion of educational platforms.

3) **Need for the bill.** As discussed in the previous section, prior to KOPIPA and ELPIPA, online companies in the preschool and K-12 education technology space could collect and sell student personal information obtained through student, parent, and teacher use of the online sites used

---

[3] Bus. & Prof. Code § 22584.
[4] Hao-Ping Lee, et al. *The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects from a Survey of Knowledge Workers*, Carnegie Mellon University (2025), *accessed at* https://www.microsoft.com/en-us/research/wp-content/uploads/2025/01/lee_2025_ai_critical_thinking_survey.pdf.

for school purposes. Because KOPIPA and ELPIPA only cover the preschool, pre-kindergarten, and K-12 students, online companies in the higher education technology space can collect and sell student personal information obtained through student, parent, and teacher use of online sites used for higher education purposes. KOPIPA was enacted to protect student personal information by closing loopholes that allowed online companies in the education technology space to profit from student personal information obtained through student, parent, teacher, and administrator use of K-12 online websites, services, and applications. The law applies to operators of such online sites, services, and applications where they have actual knowledge that they are being used primarily for K-12 school purposes and are designed or marketed for K-12 school purposes.

Concerns have arisen that certain online operators are disregarding the requirements laid out in KOPIPA over potential misinterpretations of the scope of the law's coverage. Specifically, allegations that standardized testing organizations are collecting and using student information in violation of KOPIPA's provisions.

Specifically, allegations that certain entities are disregarding the provisions of SOPIPA. The author points to a report put out by Consumer Reports, entitled "The College Board Is Sharing Student Data Once Again":

> For millions of students, the College Board is the gatekeeper to higher education. And according to a Consumer Reports investigation, the organization uses that role to collect and share information on those students—despite apparent promises to the contrary.
>
> The nonprofit company owns and operates the SAT test. It also administers the Advanced Placement exams high school students take to earn college credit and strengthen their applications. And when you create an account on collegeboard.org to register for the SAT, sign up for an AP test, or research colleges and scholarships, the College Board sends details about your activity to at least seven tech companies that profit from advertising.
>
> The list includes Adobe, Facebook, Google, Microsoft, Snapchat, Yahoo, and an advertising network called AdMedia.
>
> The personal information was relayed to these companies in a manner that appears to violate specific privacy promises made by the College Board. In some cases, it also appeared to be linked to ads for products and services beyond the organization's scope.[5]

College Board is a nonprofit organization that administers standardized tests (including the PSAT, SAT, and AP tests), primarily to high school students as part of the college admissions process. In addition, College Board operates the "Student Search" service, in which it licenses data it collects from students — including their names, contact information, ethnicity, and test

---

[5] Thomas Germain, *The College Board Is Sharing Student Data Once Again* (July 30, 2020) Consumer Reports, https://www.consumerreports.org/colleges-universities/college-board-is-sharing-student-data-once-again/#:~:text=The%20College%20Board%20is%20tracking,from%20the%20College%20Board%20website.

scores — to customers like colleges and scholarship programs to use for recruiting students.[6] College Board also provides access to the Big Future School mobile app Connections through contracts with K-12 schools.

This bill responds to these allegations by extending the protections in KOPIPA to higher education students. In addition, the bill adds an enforcement mechanism to all three laws, increases protection for sensitive information, addresses the use of student data to train AI models, and both adds and clarifies definitions. In discussing the need for the bill, the author makes a compelling point when she notes:

> Existing law fails to provide California students with comprehensive, enforceable data privacy protections. KOPIPA and ELPIPA contain exploitable ambiguities, exclude higher education students entirely, lack accessible enforcement mechanisms, and do not address contemporary threats including AI training and sensitive data collection. Federal law regulates educational institutions rather than EdTech operators and similarly lacks private enforcement.

A coalition of supporters further argue the need for the bill:

> Since KOPIPA took effect nine years ago, technology in education has accelerated rapidly. Students from preschool through university now maintain a near-constant online presence via a profusion of educational platforms. With artificial intelligence now entering classrooms and new threats to how our information is misused, modernized data protections are urgently needed. [The California Learner Personal Information Protection Act (CALPIPA)] expands protections that exist for Pre-K through 12th grade to higher education students and adds meaningful enforcement through a private right of action for affected students and families. CALPIPA also modernizes these protections by preventing EdTech companies from using student data to train AI systems, closing loopholes that have allowed companies to avoid compliance with existing privacy laws, and protecting sensitive student information related to reproductive health, immigration status, and LGBTQ+ identity.

4) **Concerns raised by the opposition.** The College Board opposes this bill. Primarily, they argue that the bill puts at risk "foundational student activities, such as sending SAT or AP scores to scholarship programs, the ability for adult learners to exercise consent over their own data, and students' ability to receive information tied directly to their in-school assessments.". Additional specific concerns from the College Board are set forth and examined below.

*The bill fails to permit essential disclosures needed for students to use their test scores for scholarships, college placement, and course credit.* KOPIPA currently allows the disclosure of covered information if it is in furtherance of the K-12 purpose and meets certain criteria. The proposed language adds an additional exception. It states that a national assessment provider – the College Board – can disclose covered information to a K-12 school, local educational agency, or higher education institution "solely for assessment, admissions, or other K-12 school purposes or higher education purposes for the benefit and use of the receiving institution."

---

[6] Jacqueline Klosek, et al. *College Board Settles for $750,000 Penalty for Sharing and Selling Student Data in Violation of New York State's Student Privacy Law*, Goodwin Data Privacy and Cybersecurity Blog, June 11, 2024 *accessed at* https://www.goodwinlaw.com/en/insights/blogs/2024/06/college-board-settles-for-750000-penalty-for-sharing-and-selling-student-data-in-violation-of-new-yo

Because sending test scores directly from the College Board to a college continues to be allowed under this bill, there is nothing that will stop a student from requesting that their test scores be sent directly to a school. In addition, nothing in this bill prevents a student from downloading their personal information and sending it directly to any institution or organization, thus ensuring that the student maintains control over their personal information. In fact, current law is very clear that nothing can prevent a student from downloading, exporting, or otherwise saving or maintaining their own personally created data and documents.[7]

*Over-regulation of college education technology.* The opposition asserts that the bill does not allow adult students to make their own informed choices as to how their data is used and to whom it is disclosed. They argue this undermines individual privacy rights. They are also concerned that the language could hinder financial aid programs that are offered to colleges and digital assessments. In addition, they argue that FERPA already governs the way the data of adult students is regulated.

This bill is in keeping with the federal prohibition against schools sharing student educational records. If a school purchases an educational tool, FERPA restricts the use of that data. Nothing in this bill conflicts with FERPA. In addition, as discussed in detail above, FERPA was not designed to address the complexities of educational technology, which is why KOPIPA, ELPIPA, and now HESIPA are necessary.

In addition, the bill does not prohibit the sale or sharing of covered information with a school or local educational agency for assessment, admissions, or other K-12 or higher education purposes. Therefore, the bill does not appear to hinder financial aid programs or digital assessments.

Finally, as mentioned above, adult students under this bill will have increased control over their test scores and other covered data because they are the only individuals who can share their information with businesses that are not covered by these laws.

*The bill's AI prohibitions could significantly hinder AI product development and classroom innovation.* The College Board argues that the prohibition on training generative AI tools with covered information "effectively bar[s] California students and educators from access to educational tools that responsibly and safely incorporate AI features." But the bill does not prohibit the use of *deidentified* personal information for such purposes. It is not clear why this limitation on the scope of information that may be used to train generative AI tools "effectively bar[s]" such tools.

*By removing the word "primarily" from the definition of "operator," the bill risks extending its reach beyond its intended focus on students in institutional settings.* However, KOPIPA and ELPIPA already contain language explicitly exempting general audience websites, online services, and applications. The bill adds the same language for HESIPA. It also clarifies the exemption in all three acts by stating that it exempts products "that are not designed or marketed" for students. Given this exemption, it is unclear how general-purpose websites that are not specifically designed or marketed for school-related purposes would be swept in.

5) **Higher Education Committee Comments.** According to the Assembly Higher Education Committee:

---

[7] Bus. & Prof. Code § 22584(o).

In the digital age, colleges and universities are asking students to utilize digital tools for educational purposes that are not controlled nor operated by the college and university. Often these educational tools, mobile apps, or digital resources, require the student to create a profile using their personal information. Since the operator of the digital service is not a college or university, the use of the student's personal information is not as protected as it would be if the tools were operated by a college or university. AB 1159 (Addis) seeks to limit the use of student personal information by non-institutional operators of a digital site, service, online application, or mobile application that is used for higher education purposes and was designed or marketed for higher education purposes. Students should not have their personal information sold or used for noneducational purposes by private operators, if the reason the student gave their personal information was to gain access to a tool for higher education purposes. While one may argue a college-age student should have the agency to determine if and when their data is shared, consent to access an educational tool is not consent for their information to be shared or sold to third parties. Disclosure of information does not equate consent and disclosure of information in order to gain access for an educational purpose does not mean consent was provided for the personal information to be used by the operate for any means. In an age where personal information is being used to provide targeted marketing in the form of advertisement or being used to evolve artificial intelligence, setting a standard to prohibit such practices for those who wish to offer digital tools for higher education purposes is reasonable. This measure appears to be a reasonable response in an age where student's personal information may be used and disclosed without the student's knowledge despite the personal information being obtained for higher educational purposes.

6) **Amendments.** The author has agreed to the following amendments to strengthen and clarify the bill:

1. In HESIPA, the sharing and sale of covered information will not only have to benefit the higher education institution, but it also must benefit the student. Similarly, in KOPIPA and ELPIPA the sharing and sale must benefit the student, parent, or teacher.

2. Clarifies in all three sections that operators or their third-party vendors can only use deidentified data to train generative artificial intelligence tools.

Due to time constraints, the amendments adopted by this Committee will be crossed by the Judiciary Committee.

***ARGUMENTS IN SUPPORT:*** Privacy Rights Clearinghouse, sponsors of the bill, write:

EdTech companies do not have a reason to be collecting a student's immigration status, sexual orientation, gender identity, or sexual and reproductive health information, and collecting this information poses real risks to students and their families.

EdTech platforms collect and share far more information than most people realize. One publisher disclosed that it receives student information from data brokers, and others have been found to share personally identifiable information, including student names and email addresses, with Google Analytics. When EdTech operators collect immigration status information along with home addresses, family contact information, and attendance patterns, that information can be disclosed, subpoenaed, or breached and put California's immigrant students and their families at risk.

> The Chronicle of Higher Education documented invasive questions about students' sexual history in required courseware for general education health courses, such as how many sexual partners the student had, whether the student used certain types of condoms and lubricants, and how frequently the student performed genital self-examinations. When students answer those questions in required assignments, in addition to being shared with their course instructor, the information becomes part of their digital educational record and may be retained by the EdTech companies.
>
> EdTech monitoring tools have also outed students to parents and administrators. A Center for Democracy and Technology survey found that nearly 30% of LGBTQ+ students reported that they or someone they knew had been outed because of online monitoring.

The sponsor further raises concerns related to using the data to train AI models:

> The granular data these platforms collect—writing samples, problem-solving approaches, learning patterns—should not be mined to build commercial AI products any more than it should be sold to data brokers. KOPIPA and ELPIPA already prohibit operators from monetizing student data through targeted advertising, data sales, and non-educational profiling. Using student data to train AI raises the same concern about commercial exploitation of information students provided for educational purposes that prompted those protections in KOPIPA and ELPIPA. AB 1159 modernizes this protection against monetizing student data by prohibiting EdTech operators from using student data to train AI systems.
>
> Major AI providers already make this commitment voluntarily to not train on student EdTech data, and the infrastructure to segregate training data from user data is well established. OpenAI's agreement with CSU includes no-training provisions. Anthropic, Microsoft, and Google offer equivalent protections in their educational products. AB 1159 makes this commitment legally required for all operators serving California students, equalizing the protections for all students rather than leaving schools to negotiate protections vendor by vendor, district by district, or hoping that companies do not change their policy.

***ARGUMENTS IN OPPOSITION:*** A coalition of business and technology organizations writes:

> TechNet and the signed organizations are strongly committed to protecting student data and privacy. The current language in print, as amended on January 5, 2025 would produce significant unintended consequences that undermine students' access to educational resources, postsecondary opportunities, and modern instructional tools.

Along with arguments that are similar to those made by the College Board and discussed in detail in Comment 4, the coalition argues:

> The addition of an expansive private right of action, without clear guardrails would expose organization to costly litigation and liability. It would divert limited resources away from educational missions and student services, discourages innovation, and could have the potential to reduce the availability of beneficial tools and programs for California students.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

Privacy Rights Clearinghouse
Asian Americans Advancing Justice Southern California
Asian Solidarity Collective
California Faculty Association
California Federation of Labor Unions, Afl-cio
California Federation of Teachers Afl-cio
California Lgbtq Health and Human Services Network
California School Employees Association
Californians Together
Cft- a Union of Educators & Classified Professionals, Aft, Afl-cio
Children's Advocacy Institute, University of San Diego School of Law
Children's Partnership, the
Consumer Action
Courage California
Gsa Network
Indivisible CA Statestrong
Oakland Privacy
Secure Justice
Students Deserve
Tech Oversight California

**Opposition**

ACT Education Corporation
California Chamber of Commerce
Computer and Communications Industry Association
College Board
TechNet

**Analysis Prepared by**: Julie Salley / P. & C.P. / (916) 319-2200