ASSEMBLY THIRD READING
AB 1159 (Addis)
As Amended January 16, 2026
Majority vote

SUMMARY

This bill creates the Higher Education Student Information Protection Act (HESIPA), which extends the protections contained in K-12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA) to higher education students. In addition, among other provisions, the bill increases privacy protections for all students.

Major Provisions

1) Creates HESIPA, which extends the protections of KOPIPA and ELPIPA to higher education students.

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

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

4) 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.

5) 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.

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

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

8) 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.

9) 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

*Need for the bill***.** 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.[1]

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 scores — to customers like colleges and scholarship programs to use for recruiting students.[2] 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.

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

---

[1] 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.
[2] 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-york

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.

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.

Arguments in Opposition
The College Board is opposed to 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." Specifically, the opponents note:

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 and the student." 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.[3]

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.

FISCAL COMMENTS

1) Possible of one-time workload costs (General Fund) for the Chancellor's Office to release guidance to students.

2) Cost pressures (Trial Court Trust Fund, General Fund) of an unknown but potentially significant amount to the courts to adjudicate cases filed by injured individuals. Actual costs will depend on the number of cases filed and the amount of court time needed to resolve each case. It generally costs approximately $1,000 to operate a courtroom for one hour. Although courts are not funded based on workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The Governor's January budget proposal for fiscal year 2026-27 provides $70 million ongoing General Fund to the Trial Court Trust Fund for court operations.

VOTES

ASM PRIVACY AND CONSUMER PROTECTION: 11-2-2
YES: Bauer-Kahan, Bennett, Bryan, Irwin, Lowenthal, McKinnor, Ortega, Patterson, Pellerin, Ward, Wicks
NO: DeMaio, Macedo
ABS, ABST OR NV: Dixon, Petrie-Norris

ASM JUDICIARY: 10-2-0
YES: Kalra, Dixon, Bauer-Kahan, Bryan, Connolly, Harabedian, Pacheco, Papan, Stefani, Zbur
NO: Macedo, Johnson

---

[3] Bus. & Prof. Code Section 22584(o).

ASM APPROPRIATIONS: 14-1-0
YES: Wicks, Hoover, Stefani, Calderon, Caloza, Fong, Mark González, Krell, Bauer-Kahan, Pacheco, Pellerin, Solache, Ta, Tangipa
NO: Dixon

UPDATED

VERSION: January 16, 2026

CONSULTANT: Julie Salley / P. & C.P. / (916) 319-2200 FN: 0002261