

CONCURRENCE IN SENATE AMENDMENTS

AB 1159 (Addis)

As Amended August 21, 2026

Majority vote

SUMMARY

This bill establishes, commencing July 1, 2027, the Higher Education Student Information Protection Act governing the collection, use, disclosure, retention, and protection of postsecondary student data by educational technology operators. It further modifies the K-12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA) to regulate the use of pupil data in artificial intelligence (AI) systems, applies their respective provisions to entities acting on behalf of an operator, and makes other changes related to protecting pupil information. It further creates a private right of action for specified violations of pupil and student privacy protection.

Senate Amendments

- 1) Revise the standards and institutional review process for operators' deidentification of student information.
- 2) Require operators to apply deidentification measures consistent with Family Educational Rights and Privacy Act (FERPA) requirements, as determined by educational institutions.
- 3) Clarify that the bill does not require educational institutions to review or approve an operator's deidentification practices.
- 4) Revise permitted sales and disclosures by national assessment providers and nonprofit enrollment-data reporting entities, subject to contractual restrictions.
- 5) Allow specified communications to students concerning course materials, payments, rentals, returns, and order fulfillment.
- 6) Extend the prelitigation notice and cure periods to 60 days.

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 Advanced Placement (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 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

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>

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 Chamber of Commerce and TechNet write in opposition to the June 18th version of the bill:

Unintended Restrictions on Educational and Postsecondary Pathways

The bill would limit the ability of students to authorize the appropriate use and disclosure of their own educational information for essential purposes, such as applying for scholarships, qualifying for college placement or academic credit, accessing financial aid, and receiving information about postsecondary and workforce opportunities. By restricting these pathways, the bill would disproportionately impact students who rely on opt-in services and data-enabled tools to navigate higher education and career options.

Barriers to Responsible Innovation

The bill's prohibitions on artificial intelligence and data use would significantly hinder the development and deployment of responsible, education-focused technologies. Data is essential to improving instructional tools, assessment systems, and accessibility features. Preventing the use of appropriately safeguarded education data for product improvement and

innovation would slow progress in classrooms and conflict with how modern educational tools are designed and used.

Private Right of Action

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.

FISCAL COMMENTS

According to the Senate Appropriations Committee analysis, this bill would have the following fiscal impact:

- 1) This bill could result in additional, unknown cost pressures to the courts to adjudicate additional cases that are filed. The actual costs will depend on the number of cases filed and the amount of court time needed to resolve each case. It typically costs about \$1,000 to operate a courtroom for one hour. Although the courts are not funded based on workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for the courts from the General Fund.
- 2) The Chancellor's Office estimates minor, one-time Proposition 98 General Fund costs for the community colleges to train staff on student rights under the Higher Education Student Information Protection Act. There could also be one-time General Fund workload costs of \$12,000 to \$23,000 for the Chancellor's Office to release guidance.
- 3) The administrative costs to the University of California and California State University are expected to be minor and absorbable within existing resources.
- 4) The Department of Justice anticipates no significant fiscal impact as a result of this measure.

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

ASM APPROPRIATIONS: 14-1-0

YES: Wicks, Hoover, Stefani, Calderon, Caloza, Fong, Mark González, Krell, Bauer-Kahan, Pacheco, Pellerin, Solache, Ta, Tangipa

NO: Dixon

ASSEMBLY FLOOR: 65-5-10

YES: Addis, Aguiar-Curry, Ahrens, Alanis, Alvarez, Ávila Farías, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Chen, Connolly, Davies, Elhawary, Fong, Gabriel, Garcia, Gipson, Jeff Gonzalez, Mark González, Haney, Harabedian, Hart, Hoover, Irwin, Jackson, Kalra, Krell, Lee, Lowenthal, McKinnor, Muratsuchi, Nguyen, Ortega, Pacheco, Patel, Patterson, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Ransom, Michelle Rodriguez, Rogers, Blanca Rubio, Sanchez, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Valencia, Wallis, Ward, Wicks, Wilson, Zbur, Rivas

NO: DeMaio, Ellis, Johnson, Macedo, Tangipa

ABS, ABST OR NV: Arambula, Castillo, Dixon, Flora, Gallagher, Hadwick, Lackey, Papan, Celeste Rodriguez, Ta

UPDATED

VERSION: August 21, 2026

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

FN: 0004537