Date of Hearing: January 15, 2026

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
AB 1159 (Addis) – As Amended January 5, 2026

As Proposed to be Amended

SUBJECT: STUDENT PERSONAL INFORMATION

KEY ISSUE: SHOULD CALIFORNIA STRENGTHEN ITS STUDENT PRIVACY LAWS BY EXPRESSLY LIMITING THE USE OF STUDENT DATA IN ARTIFICIAL INTELLIGENCE SYSTEMS, EXTENDING EXISTING K–12 AND EARLY-LEARNING DATA PROTECTIONS TO HIGHER EDUCATION, AND AUTHORIZING PRIVATE ENFORCEMENT?

SYNOPSIS

Existing California law provides sector-specific protections for student data in K–12 and early-learning contexts through the K–12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA), but those statutes were enacted before the widespread use of artificial intelligence in education and do not extend comparable safeguards to higher education students. As educational technology has become ubiquitous both inside and outside the classroom—and increasingly reliant on large-scale data collection and analytics—students now face heightened risks that their personal information may be repurposed for noneducational, commercial uses, including the training of artificial intelligence systems. According to the author, ambiguities in existing law, gaps in coverage for college and university students, and outdated substantive protections for sensitive categories of data have left millions of California learners without adequate privacy safeguards. This bill responds to those concerns by modernizing and harmonizing California's student data privacy framework, expressly limiting the use of student information in artificial intelligence systems, extending KOPIPA-style protections to higher education, and strengthening enforcement through a calibrated private right of action with a notice-and-cure mechanism designed to promote compliance while avoiding unnecessary litigation. This measure was preciously heard and approved by the Committee on Privacy and Consumer Protection. The bill is sponsored by the Privacy Rights Clearinghouse and is supported by a broad coalition of labor organizations, tech oversight and consumer protection groups and children's advocacy organizations. College Board and ACT Education Corporation oppose this measure. The proposed author's amendments are reflected in the SUMMARY below and throughout this analysis. The bill will be heard in the Privacy & Consumer Protection Cmte prior to this hearing.

SUMMARY: Extends California's student data privacy framework to artificial intelligence uses and higher education and authorizes private enforcement. Specifically, **this bill**:

1) Expands the scope of the K–12 Pupil Online Personal Information Protection Act (KOPIPA) to expressly regulate the use of pupil data in artificial intelligence systems by prohibiting operators from using covered information, including persistent unique identifiers, to train or develop artificial intelligence systems unless the use is strictly in furtherance of K–12 school purposes and for the use and benefit of the school and the teacher, pupil, or parent.

2) Expands the scope of the Early Learning Personal Information Protection Act (ELPIPA) to impose parallel restrictions on the use of preschool and prekindergarten pupil data in artificial intelligence systems, subject to the same purpose and benefit limitations applicable to early learning programs.

3) Broadens and modernizes the definition of "covered information" under KOPIPA and ELPIPA to expressly include additional categories of data commonly collected by digital education platforms, including behavioral information, device identifiers, extracurricular activities, and similar data elements.

4) Clarifies and standardizes definitions related to artificial intelligence, including "artificial intelligence," "generative artificial intelligence," and "training a generative artificial intelligence system or service," by cross-reference to Civil Code section 3110, to ensure consistency across California privacy statutes.

5) Enacts the Higher Education Student Information Protection Act (HESIPA) to extend KOPIPA-like privacy protections to students enrolled in higher education institutions, including colleges, universities, vocational programs, and postgraduate programs.

6) Prohibits operators serving higher education students from engaging in targeted advertising, profiling, sale of student information, or use of covered information to train artificial intelligence systems, except where such use is in furtherance of higher education purposes and for the use and benefit of the higher education institution and the student.

7) Prohibits, without exception, the collection, use, retention, or disclosure of certain highly sensitive categories of student data in the higher education context, including information relating to reproductive or sexual health, immigration status, precise geolocation, and sexual orientation or gender identity.

8) Imposes data security, retention, deletion, and disclosure obligations on operators subject to KOPIPA, ELPIPA, and HESIPA, including requirements to maintain reasonable security procedures, delete covered information upon request in specified circumstances, and retain data only as long as reasonably necessary for the applicable educational purpose.

9) Creates an express private right of action authorizing a pupil, student, or their parent or guardian who suffers actual harm as a result of an operator's noncompliance with KOPIPA, ELPIPA, or HESIPA to bring a civil action against the operator.

10) Authorizes statutory and equitable remedies in a private action, including the greater of actual damages or five hundred dollars ($500) per plaintiff per violation, injunctive relief, punitive damages, and reasonable attorney's fees and costs.

11) Establishes a notice-and-cure requirement requiring a prospective plaintiff to provide at least 45 days' written notice of the alleged violation and an opportunity for the operator to correct and remedy the violation before filing suit, with successful cure barring certain individual and class actions.

12) Delays the operative date of the Higher Education Student Information Protection Act until July 1, 2027.

EXISTING LAW:

1) Regulates the collection, use, retention, and disclosure of K–12 pupil data by educational technology operators through the K–12 Pupil Online Personal Information Protection Act (KOPIPA), which applies to operators of internet websites, online services, online applications, or mobile applications designed and marketed for K–12 school purposes and used with actual knowledge of such use. (Business and Professions Code Section 22584(a). All further statutory references are to the Business and Professions Code, unless otherwise specified.)

2) Prohibits operators subject to KOPIPA from engaging in targeted advertising, profiling, or sale of pupil information, except as expressly permitted, including prohibitions on targeted advertising based on covered information, amassing profiles of pupils outside K–12 school purposes, and selling covered information subject to limited transactional exceptions. (Section 22584(b).)

3) Restricts disclosure of K–12 pupil covered information to specified circumstances, including disclosures in furtherance of K–12 school purposes, for legal or regulatory compliance, in response to judicial process, to protect safety or security, or to service providers operating under contractually imposed data-use and security limitations. (*Id*.)

4) Requires operators subject to KOPIPA to implement reasonable data security practices and data governance safeguards, including maintaining reasonable security procedures, deleting pupil information upon request by a school or local educational agency, limiting retention to what is reasonably necessary for the purpose collected, and maintaining a written data retention policy. (Section 22584(d).)

5) Excludes certain pupil data from the California Consumer Privacy Act of 2018 (CCPA) by defining "CCPA-excluded covered information" and expressly regulating such data under KOPIPA instead of Title 1.81.5 of Part 4 of Division 3 of the Civil Code. (Section 22584(a); Civil Code Section 1798.100 *et seq*.)

6) Extends substantially similar protections to preschool and prekindergarten pupils through the Early Learning Personal Information Protection Act (ELPIPA), which regulates operators of online services designed and marketed for preschool or prekindergarten purposes and imposes parallel prohibitions on targeted advertising, profiling, sale, and improper disclosure of covered information. (Section 22586(a), (b).)

7) Imposes data security, deletion, and retention obligations on operators subject to ELPIPA, including requirements to implement reasonable security procedures, delete covered information upon request in specified circumstances, retain data only as long as reasonably necessary, and maintain a written data retention policy. (Section 22586(d).)

8) Limits enforcement of KOPIPA and ELPIPA primarily to public enforcement, with no express statutory private right of action authorizing pupils, students, or parents to bring civil actions for violations, and no provision for statutory damages or attorney's fees. (Sections 22584, 22586.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Assembly Bill 1159 (the California Learner Personal Information Protection Act, or CALPIPA) updates California's student data privacy framework in light of dramatic technological changes that have outpaced existing law. When the Student Online Personal Information Protection Act, now known as the K–12 Pupil Online Personal Information Protection Act (KOPIPA), was enacted in 2014, the Legislature was responding to the growing use of educational technology in K–12 classrooms and the emerging risks associated with internet-connected learning tools. At that time, student technology use was largely confined to discrete classroom applications, and the Legislature sought to prevent the commercialization of student data by imposing baseline restrictions on education technology vendors, including prohibitions on the sale of student data, targeted advertising, non-educational profiling, and unauthorized disclosure, as well as requirements to implement reasonable data security practices.

Since KOPIPA took effect in 2016, however, the educational technology landscape has changed fundamentally. Students from preschool through university now maintain a near-constant digital presence across multiple platforms used both inside and outside the classroom, often on personal devices and in home settings. The author explains:

> 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.

Existing law. Under existing law, student data privacy in California is governed by a patchwork of federal and state statutes that allocate regulatory responsibility across multiple legal regimes and legislative committees. At the federal level, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) regulates the disclosure of education records by educational agencies and institutions receiving federal funds, but generally does not apply to private educational technology vendors except through contractual arrangements with schools, nor does it directly regulate commercial uses of student data. At the state level, California has enacted sector-specific student privacy statutes—including the K–12 Pupil Online Personal Information Protection Act (Business and Professions Code Section 22584) enacted in 2014 by Senate Bill 1177 (Steinberg) (Stats. 2014, Chap. 839), codified at Business and Professions Code sections 22584–22585, in response to the rapid adoption of cloud-based and digital learning tools in K–12 classrooms and the Legislature's determination that federal law, particularly FERPA, did not adequately regulate private operators' use of pupil information; the statute therefore prohibits targeted advertising, profiling, and sale of pupil data, restricts disclosure to narrow educational and legal purposes, and imposes data security, retention, and deletion obligations, all with the central aim of preventing commercial exploitation of pupil information while permitting use solely for K–12 school purposes and for the benefit of schools and pupils. Building on that framework, the Legislature enacted ELPIPA in 2016 through Assembly Bill 2799 (Chau) (Stats. 2020, Chap. 620), codified at Business and Professions Code section 22586, to extend substantially similar protections to preschool and prekindergarten children, recognizing that early-learning platforms increasingly collect highly sensitive developmental and behavioral data

from children who lack legal capacity to consent and were not covered by KOPIPA or the California Consumer Privacy Act; ELPIPA mirrors KOPIPA's prohibitions on targeted advertising, profiling, and sale of covered information, as well as its limits on disclosure, security, and retention, to ensure continuity of privacy protections from early learning through K–12. Together, KOPIPA and ELPIPA demonstrate a consistent legislative intent to treat student data privacy as a distinct regulatory domain—separate from general consumer privacy law—focused on limiting secondary commercial uses of educational data by private operators, an intent that has continued to evolve through subsequent amendments addressing new technologies, enforcement gaps, and the expansion of digital education tools.

In sum, these statutes reflect a decade-long legislative effort by the California Legislature to address the growing collection and commercialization of student data by private educational technology vendors operating outside the scope of traditional education privacy laws.

Significantly, both existing statutes provide for enforcement only through Attorney General action.

What the bill does – Enhanced Protections re Artificial Intelligence. This bill modernizes California's student data privacy framework by expressly regulating the use of student personal information in artificial intelligence systems. Existing student privacy statutes—KOPIPA and ELPIPA—were enacted before the widespread deployment of generative AI and large-scale data analytics in educational technology and do not explicitly address whether, or under what circumstances, student data may be used to train or develop AI models. AB 1159 closes that gap by clarifying that covered student information, including persistent unique identifiers, may not be used to train or develop artificial intelligence systems unless the use is strictly in furtherance of an educational purpose and for the use and benefit of the relevant educational institution. The bill also strengthens protections for sensitive categories of student data, including information relating to immigration status, reproductive or sexual health, and sexual orientation or gender identity, reflecting the heightened risks posed by advanced data aggregation and inference technologies.

Existing law permits disclosure of covered information when "necessary to ensure legal and regulatory compliance" and "to protect the safety of users or others or security of the site," raising concerns that the vague language might enable law enforcement to inappropriately access covered information. To further protect students and their families from inappropriate sharing of covered information between operators and law enforcement, the author may wish to consider amending the bill to limit the disclosure exception to lawful compliance with a court order.

What the bill does – Extends Student Data Protection to Higher Education. AB 1159 extends comprehensive student data privacy protections beyond K–12 and early learning by enacting the Higher Education Student Information Protection Act, thereby creating a unified privacy framework that applies from preschool through postsecondary education. While ELPIPA extended KOPIPA-like safeguards to preschool and prekindergarten students, higher education students—numbering approximately 2.9 million in California—remain largely outside any comparable state-level statutory regime governing the conduct of educational technology vendors. The bill fills this gap by applying core KOPIPA protections to higher education contexts, including prohibitions on targeted advertising, profiling, sale of student data, and improper disclosure, while also imposing heightened restrictions on the collection and use of

particularly sensitive information. In doing so, the bill recognizes that college and university students face similar, and in some cases greater, risks of data misuse due to the scale, persistence, and sensitivity of information collected through modern digital learning platforms.

What the bill does – Provides for a private right of action with notice to cure provision. AB 1159 significantly strengthens enforcement of California's student data privacy laws by establishing a limited private right of action for students, pupils, or their parents or guardians who suffer actual harm as a result of an operator's noncompliance with KOPIPA, ELPIPA, or the new higher education provisions, while simultaneously incorporating a structured notice-and-cure framework designed to promote compliance and avoid unnecessary litigation. Under existing law, KOPIPA and ELPIPA have relied exclusively on the Attorney General for enforcement, resulting in only a single enforcement action in nearly a decade. The November 2025 Illuminate Education case, California's first KOPIPA enforcement, involved a 2021 data breach that affected millions of California students. (*Attorney General Bonta Joins States in Securing $5.1 Million in Settlements from Education Software Company for Failing to Protect Students' Data*, available at https://oag.ca.gov/news/press-releases/attorney-general-bonta-joins-states-securing-51-million-settlements-education.)

According to the author, this model has proven insufficient given the scale and complexity of the educational technology market, the rapid evolution of data practices, and the fact that many violations occur within proprietary systems that are difficult for regulators to detect. As a result, students and families who suffer actual harm from unlawful data practices often lack a meaningful remedy.

AB 1159 addresses this gap by authorizing a pupil, student, or their parent or guardian who has suffered actual harm as a result of an operator's noncompliance to bring a civil action seeking actual or statutory damages, injunctive relief, punitive damages where appropriate, and reasonable attorney's fees and costs, while conditioning access to the courts on compliance with a detailed pre-litigation process.

Central to this enforcement scheme is the bill's notice-and-cure requirement, which requires a prospective plaintiff to provide written notice identifying the alleged violations and affords the operator a defined period to cure the noncompliance before any action may be filed. If the operator fully remedies the violation within the cure period and provides appropriate relief, the statute bars the plaintiff from maintaining an individual or class action based on the cured conduct. For class actions, the bill further requires a showing that the operator failed to cure violations affecting similarly situated students, ensuring that class litigation is reserved for systemic or willful noncompliance rather than isolated or technical errors. This structure reflects the author's intent to make private enforcement remedial rather than punitive, incentivizing prompt correction of unlawful data practices while deterring opportunistic litigation.

AB 1159's private right of action is modeled directly on the California Student Borrower Bill of Rights (AB 376 (Stone), Chap. 154, Stats. 2020), codified at Civil Code Section 1788.103, which similarly authorizes private enforcement while prioritizing notice, remediation, and good-faith compliance. Under the borrower protections, servicers are afforded an opportunity to correct violations once notified, and successful cure limits or precludes liability, a structure that has been recognized as balancing consumer protection with regulatory certainty. By adopting a parallel approach, AB 1159 places student data privacy enforcement within an established California

statutory model that treats violations as correctable regulatory failures rather than automatic triggers for litigation.

Author's Amendments. The author proposes the following amendments to ensure that covered information used to train generative artificial intelligence is deidentified, and make confirming changes:

Section 22584 (a)(10)

"Operator" means the ~~**operator**~~ ***operator, or an entity working on behalf of the operator,*** of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes and was designed or marketed for K–12 school purposes, including a provider of digital educational software or services, including digital course books.

Similar changes will be made to the definition of "operator" throughout the bill.

Section 22586(b) An operator shall not knowingly engage in any of the following activities with respect to the operator's site, service, or application:

(5) Use covered information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to train ~~***an***~~ ***a*** generative artificial intelligence system or service or develop an artificial intelligence system.

The author also proposes amendments to the existing KOPIPA and ELPIPA statutes to require that the sharing and sale of covered information not only has to benefit the higher education institution, but it also must benefit the student, parent, or teacher.

Section 22584(b) An operator shall not knowingly engage in any of the following activities with respect to the operator's site, service, or application:

(2) Use any information, including covered information and persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a pupil enrolled in a local educational agency, except in furtherance of K–12 school purposes and for the use and benefit of the K–12 school ***and the teacher, pupil, or parent.***

Section 22586(b) An operator shall not knowingly engage in any of the following activities with respect to the operator's site, service, or application:

(2) Use any information, including covered information and persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a pupil enrolled in a local educational agency, except in furtherance of K–12 school purposes and for the use and benefit of the K–12 school ***and the teacher, pupil, or parent.***

And amendments to HESIPA to require that the sharing and sale also benefits the student:

Section 22587 (b) An operator shall not knowingly engage in any of the following activities with respect to the operator's site, service, or application:

(3) Sell a student's information, including covered information, unless the sale meets either of the following criteria:

(A) The sale is for the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.

(B) The sale is made by a national assessment provider 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.***

…

(4) Disclose covered information unless the disclosure meets any of the following criteria:

…

(F) The disclosure is by a national assessment provider to a higher education institution, or K–12 school or local educational agency, as defined in Section 22584, solely for assessment, admissions, or other higher education purposes or K–12 school purposes, as defined in Section 22584, for the use and benefit of the receiving institution ***and the student.***

ARGUMENTS IN SUPPORT*:* Privacy Rights Clearinghouse, the sponsor of this measure explains the need for the private right of action:

> KOPIPA and ELPIPA have relied exclusively on the Attorney General for enforcement. The Attorney General's office has limited resources and cannot pursue every violation, resulting in only one enforcement action in nearly a decade. This lack of enforcement provides no incentive for EdTech companies to follow the law. When people have rights on paper but no practical way to vindicate them, they lose faith that the system works for them at all. Research on legal cynicism ties this erosion to people experiencing law as something that happens to them rather than for them.
>
> AB 1159 therefore creates a narrow, very limited private right of action focused on ensuring compliance with the law. It has nearly identical provisions to the Student Borrower Bill of Rights (Civil Code Section 1788.103), which Governor Newsom signed in 2020 with support from 70 civil rights, higher education, and consumer advocacy organizations and which has not resulted in abusive litigation. Students must provide 45 days' written notice before filing suit, giving operators the opportunity to cure. Individual actions are blocked if operators correct violations within 30 days. Class actions face additional guardrails. Compliance efforts cannot be used as admission of wrongdoing. Students must still allege actual harm to have standing.
>
> Students should not be in a position where completing a required assignment puts them or their families at risk. AB 1159 updates California's student privacy framework to address the modern challenges students face while preserving the structure California pioneered a decade ago. For these reasons, we are proud to sponsor AB 1159.

ARGUMENTS IN OPPOSITION*:* The College Board opposes this measure, arguing that the bill places 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 assessment. The College Board also opposes the private right of action, arguing:

> The express addition of the private right of action subjects Operators to class action and other litigation exposure, which presents an extraordinary expense that limit College Board's ability to dedicate nonprofit resources to our educational mission, and by extension, limits resources that can be made available to students. The expansiveness of the bill's language, which does not include Attorney General enforced guardrails, invites lawsuits by opportunistic litigants seeking to extract settlements from companies developing and offering educational products that serve the public interest and that the Legislature never intended to discourage when passing this landmark legislation over a decade ago.

REGISTERED SUPPORT / OPPOSITION:

Support

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
Privacy Rights Clearinghouse
Secure Justice
Students Deserve
Tech Oversight California

Opposition

ACT Education Corporation
College Board

Analysis Prepared by: Shiran Zohar / JUD. / (916) 319-2334