SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 1159 (Addis)
Version: January 16, 2026
Hearing Date: June 22, 2026
Fiscal: Yes
Urgency: No
BH

SUBJECT

Student personal information

DIGEST

This bill enacts the Higher Education Student Information Protection Act (HESIPA) which extends the general protections of student privacy found in the K-12 Pupil Online Personal Information Protection Act (KOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA). This bill authorizes a pupil or student actually harmed by the noncompliance with KOPIPA, ELPIPA, or HESIPA to bring a civil action against the noncompliant operator, as specified.

EXECUTIVE SUMMARY

Privacy protections for California's students are contained primarily within KOPIPA and ELPIPA. These protections, however, cover very young students in early education (ELPIPA), with elementary and high school students covered by KOPIPA. This bill extends the privacy protections in place for younger students to students attending college. Protections for college students have lagged behind as courseware, digital textbooks and online materials have made these students increasingly vulnerable to inappropriate data collection and privacy issues.

The bill is sponsored by the Privacy Rights Clearinghouse, working to protect college student privacy. The bill is opposed by technology companies that argue this would restrict how operators may use certain student information and would authorize students to bring a private right of action. The bill passed out of the Senate Education Committee on a vote of 4 to 0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights regarding 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. (Civil Code (CIV) § 1798.100 et seq.)

2) 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. Prohibits 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. (Busn. & Prof. Code §§ 22584, 22584(b)).

3) Establishes the ELPIPA, which extends the protection of KOPIPA to pupils in preschool and prekindergarten. (Busn. & Prof. Code § 22586).

4) 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. § 6501; 16 C.F.R. Part 312).

5) 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).

This bill:

1) Expands the scope of KOPIPA to regulate the use of pupil data in AI systems by prohibiting operators from using covered information, including persistent unique identifiers, to train or develop AI systems unless the use is 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 ELPIPA to regulate the use of pupil data in AI systems by prohibiting operators from using covered information, including persistent unique identifiers, to train or develop AI systems unless the use is strictly in furtherance of

preschool or prekindergarten purposes and for the use and benefit of the preschool or prekindergarten and the teacher, pupil, or parent.

3) Establishes, operative July 1, 2027, the Higher Education Student Information Protection Act to regulate the collection, use, disclosure, and protection of postsecondary education student data by educational technology operators, as defined. Specifically, it:
    a) Prohibits operators from knowingly engaging in targeted advertising based on student information, creating student profiles unrelated to higher education purposes, selling student information except in limited circumstances, making unauthorized disclosures of covered information, or using covered information to train or develop AI systems, as specified.
    b) Prohibits operators from collecting, using, retaining, or disclosing specified categories of sensitive student information, including information relating to reproductive or sexual health, immigration status, precise geolocation, and sexual orientation or gender identity, as specified.
    c) Specifies circumstances under which disclosures of covered information are not prohibited, including higher education purposes, research, legal compliance, security, and contracted services providers, subject to certain conditions, as specified
    d) Requires operators to implement and maintain reasonable security procedures and data governance practices. Operators are to protect student information from unauthorized access or disclosure, comply with specified student and institutional requests to delete covered information, limit retention of covered information to the period reasonably necessary to fulfill its purposes, and maintain a written data retention policy that identifies retention and deletion timelines, as specified.
    e) Specifies various exemptions and permitted uses of student information, including the use of deidentified or aggregated information for product improvement and research, adaptive learning and customized instruction, and disclosures otherwise authorized by law, as specified.
    f) Clarifies that the bill's provisions do not supersede specified federal student privacy and disability laws.

4) Creates a private right of action for specified violations of pupil and student privacy protections.

5) Expands the definition of "covered information" under KOPIPA and ELPIPA to include additional categories of information, including extracurricular activities, biometric or behavioral information, device identifiers, search activity, photographs, and voice recordings. The bill applies a similar definition under the Higher Education Student Information Act.

6) Expands the definition of "Operator" under KOPIPA and ELPIPA to include entities working on behalf of operators of websites, online services, applications, or online applications designed, marketed, and used for educational purposes, including providers of digital educational software and services. The bill applies a similar definition under the Higher Education Student Information Protection Act.

COMMENTS

1. A constitutional imperative

   It is instructive to note that the Senate Education Committee analysis reminded us that privacy is a constitutional imperative. The full text of Article 1, Section 1 of the California Constitution is as follows:

   "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and **privacy**" (emphasis added).

   This bill, by extending privacy protections to college students, furthers that constitutional requirement.

2. Expands protection to college students

Privacy protections for California's students are contained primarily within KOPIPA and ELPIPA. These protections, however, cover very young students in early education (ELPIPA), with elementary and high school students covered by KOPIPA. This bill extends the privacy protections in place for younger students to students attending college. Protections for college students have lagged behind as courseware, digital textbooks, and online materials have made these students increasingly vulnerable to inappropriate data collection and privacy issues.

3. The cost of access

In its report, "Paying Twice to Learn," the Privacy Rights Clearinghouse concludes: "Students disclose personal information while doing coursework required by a professor for a class that they pay for, using a textbook that they pay for (directly or indirectly). What happens to that personal information - whether it is appropriately protected, further monetized for other commercial purposes, or disclosed to additional parties for additional uses - is hard to decipher."

All students, regardless of age, have a reasonable expectation the college courseware they are required to purchase in an educational environment is covered by the same privacy protections provided younger students from early learning to high school

matriculation. This bill seeks to achieve consistent privacy policy protections across all educational levels.

4. No equivalent protection

The author argues that currently, there are no equivalent protections for college students. The author has provided the following statement.

> 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 at California's higher education institutions have no equivalent protection. AB 1159, the CA Learner Personal Information Protection Act, modernizes existing data protections in the education field and extends those protections to higher education students, ensuring that *all* students can learn safely and securely in an increasingly digital world.

This bill expands existing K-12 and early learning student privacy laws while establishing a new higher education privacy framework. Although many provisions are substantially similar across the three acts, the bill creates separate statutory frameworks governing different educational sectors.

5. Arguments in support

Privacy Rights Clearinghouse, the sponsor, writes:

> Today, students face never-before-seen threats to their privacy in the classroom. The California Learner Personal Information Protection Act (CALPIPA) ensures that California's 6.9 million K-12 and 2.5 million higher education students have strong, comprehensive privacy protections that reflect modern technological realities and the ways our information is being weaponized against us.
>
> CALPIPA ensures that information collected from any California student for educational purposes is used only for educational purposes and cannot be misused by Big Tech. It builds on existing student privacy laws, clarifying and expanding their protections and modernizing them to account for new threats to student privacy. For these reasons, we are proud to support AB 1159.

UnidosUS writes in support:

> Assembly Bill 1159 both updates and expands existing student data protections through four main actions. First, it clarifies the existing definitions of "operator", "school purpose" and "general audience" to protect students in the classroom and at home when accessing EdTech. Second, it creates higher education privacy safeguards for California's 2.9 million college and university students while improving both KOPIPA and ELPIPA, ensuring a comprehensive privacy framework across all educational levels. Third, it sets reasonable limits on data sharing and retention, with protections for sensitive information (immigration status, LGBTQ+ identity, reproductive health), and prohibits businesses from using student data to train GenAI models. Lastly, it establishes a private right of action with safeguards, including 45-day notice and cure periods.
>
> For these reasons, we respectfully request your support for AB 1159 and appreciate your consideration of this important legislation.

6. Arguments in opposition

CalChamber, Technet, and the Computer and Communications Industry Association in opposition argue:

> **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.

This bill creates a private right of action for specified violations of its student privacy protections. This committee will consider the students' private right of action as part of the structural protection of student privacy.

7. Possible author's amendments

The author's office continues to refine the bill, working with affected parties, and has provided the following list of possible future amendments:

- Update the definition of de-identified information to clarify that de-identification measures must meet or exceed FERPA requirements.
- Give schools oversight over de-identification if they would like, ensuring schools have oversight for FERPA compliance without putting a mandate on schools.
- Require operators follow de-identification policies and standards that meet or exceed a school's policy or standard.
- Provide an enforcement option for schools to stop providing student information if an operator does not properly de-identify.
- Update the definition of operator to clarify that an operator does not include schools and districts.
- Fix a drafting error so the definition of operator is consistent across all PIPAs.
- Add PRA notice requiring someone filing a PRA provide notice to the AG when filing. This would still allow the AG to weigh in if they think the lawsuit is baseless without burdening them with additional oversight.

SUPPORT

Privacy Rights Clearinghouse (sponsor)
Alliance of Californians for Community Empowerment (ACCE) Action
Asian Americans Advancing Justice Southern California
Asian Solidarity Collective
CA Now
California Faculty Association
California Federation of Labor Unions, AFL-CIO
California LGBTQ Health and Human Services Network
California National Organization for Women
California Nurses Association
California Police Chiefs Association
California School Employees Association
California State PTA
California Work & Family Coalition
Californians Together
CFT – a Union of Educators & Classified Professionals, AFT, AFL-CIO

Children's Advocacy Institute
Children's Partnership
Common Sense Media
Consumer Action
Consumer Federation of California
Courage California
Dental Board of California
Equal Rights Advocates
Genders & Sexualities Alliance Network
GSA Network
Indivisible CA Statestrong
Kapor Center Advocacy
Lieutenant Governor Eleni Kounalakis
Nextgen California
Oakland Privacy
Secure Justice
Students Deserve
Tech Oversight California
Techequity Action
Unidosus

OPPOSITION

California Association of College Stores
California Chamber of Commerce
College Board
Computer & Communications Industry Association
National Association of College Stores
Technet

RELATED LEGISLATION

SB 1177 (Steinberg, 2014) created the Student Online Personal Information Protection Act (SOPIPA). Established California's first vendor-focused student-privacy law making California a national leader on student data privacy.

AB 2799 (Chau, 2016) extended SOPIPA's protections to preschool and prekindergarten pupils through the Early Learning Personal Information Protection Act (SOPIPA), effective July 1, 2017.

AB 801 (Patterson, 2024) renamed SOPIPA to the K-12 Pupil Online Personal Information Protection Act (KOPIPA), changed terminology from "student" to "pupil," and added deletion rights for information not covered by the CCPA.

AB 1971 (Addis, 2024) was introduced to expand KOPIPA to cover standardized testing organizations and remove the "general audience" exemption. Industry opposition narrowed the enacted version to a separate chapter rather than amending KOPIPA itself.

PRIOR VOTES:

Assembly Floor (Ayes 65, Noes 5)
Assembly Appropriations Committee (Ayes 14, Noes 1)
Assembly Judiciary Committee (Ayes 10, Noes 2)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 2)

****