



December 22, 2025

The Honorable Dawn Addis
1021 O Street, Suite 4120
Sacramento, CA 95814

RE: AB 1159 – as will be amended in Assembly Privacy & Consumer Protection
Committee
SPONSOR

Dear Assemblymember Addis,

Privacy Rights Clearinghouse is proud to sponsor AB 1159, the California Learner Personal Information Protection Act (CALPIPA). California's 2014 Student Online Personal Information Protection Act (now known as KOPIPA) established the national model for student data privacy, with more than twenty states following California's lead. In 2016, California extended those protections to preschool and prekindergarten students through the Early Learning Personal Information Protection Act (ELPIPA). AB 1159 continues that approach: it updates both KOPIPA and ELPIPA to address gaps that have emerged over the past decade, including extending equivalent protections to higher education students using the same structure focused on educational technology (EdTech) companies. Specifically, CALPIPA clarifies the scope of KOPIPA and ELPIPA, establishes safeguards for sensitive information, ensures student data cannot be monetized through training AI, extends protections to higher education students, and boosts compliance incentives.

Protecting Sensitive Information

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.

AB 1159 ensures EdTech operators cannot collect this sensitive information in the first place. AB 1159 prohibits EdTech operators from collecting, using, retaining, or disclosing especially sensitive student information: immigration status, reproductive or sexual health information, sexual orientation, and gender identity.

Prohibiting AI Training on Student Data

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. KOIPA and ELIPA 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 KOIPA and ELIPA. 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.

Extending Protections to Higher Education

California's 2.9 million higher education students currently lack any equivalent to KOIPA's protections. The justification for protecting younger students applies with equal need here: students cannot meaningfully consent to data practices when the alternative is losing access to required course materials.

When California recognized that early learners faced the same privacy risks as K-12 students, the Legislature responded with ELIPA, mirroring KOIPA's substantive framework for preschool and prekindergarten. Higher education students have waited nearly a decade for equivalent treatment. This gap also affects high school students taking college courses for dual credit, who lose KOIPA's protections the moment they log into a higher education platform.

AB 1159 creates the Higher Education Student Information Protection Act (HESIPA), extending parallel protections to college and university students.

Clarifying Scope

Operators collecting EdTech data from students have found ways to escape ELPIPA and KOPIPA's requirements. Under current law, an "operator" is a service that is used "primarily" for educational purposes and was "designed and marketed" for those purposes. Operators have exploited both phrases to say they are not EdTech companies subject to the law, even while pitching to school districts, setting up booths on campuses, and knowing that schools use their products.

AB 1159 addresses these definitional loopholes and makes a similar change to the definition of "general audience" for the same reason: an operator cannot claim to not be an EdTech operator if it either designed or marketed its product for schools. These changes do not expand the law beyond its original intent. They ensure operators cannot escape compliance through arguments that have nothing to do with the privacy risks students face.

Ensuring Compliance

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.

Sincerely,

Emory Roane
Associate Director of Policy
Privacy Rights Clearinghouse

CC: Members and Staff, Assembly Privacy & Consumer Protection Committee
Members and Staff, Assembly Judiciary Committee