Date of Hearing: June 16, 2026

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 930 (Reyes) – As Amended March 25, 2026

SENATE VOTE: 37-0

SUBJECT: Student Test Taker Privacy Protection Act: end-to-end encryption

SYNOPSIS

During the COVID-19 pandemic, schools increasingly relied on remote proctoring tools capable of collecting sensitive information such as biometric data, identification documents, browsing history, video and audio recordings, and information about a student's surroundings. While student privacy is protected under both federal and state law, recent reports of data breaches and security vulnerabilities involving educational technology companies have heightened concerns that vendors continue to retain large amounts of sensitive student information.

SB 930 requires businesses providing proctoring services to local educational agencies for classroom- or course-based exams to use end-to-end encryption to provide such services. By ensuring that data transmitted through proctoring software is unreadable to the proctoring service provider, this bill seeks to mitigate the risk of unauthorized access, interception, or misuse of sensitive student information.

SB 930 is sponsored by the First Day Foundation and Los Amigos de la Comunidad. It is supported by a variety of educators, privacy advocates, and proctoring service providers, including the California Teachers Association, Oakland Privacy, and Proctorio. The bill has no registered opposition.

If passed by this committee, the bill will next be heard by the Assembly Education Committee.

EXISTING LAW:

1) Defines the following terms:

    a. "Personal information" to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. States that personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

        i. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

        ii. Any personal information described in Section 1798.80(e).

iii. Characteristics of protected classifications under California or federal law.

iv. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

v. Biometric information.

vi. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

vii. Geolocation data.

viii. Audio, electronic, visual, thermal, olfactory, or similar information.

ix. Professional or employment-related information.

x. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act. (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

xi. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

xii. Sensitive personal information. (Civ. Code § 1798.140(v).)

b. "Proctoring services" to include, but not be limited to, services offered by a business to observe, monitor, or administer an exam. (Bus. & Prof. Code § 22588.)

2) Requires, pursuant to the federal Family Educational and Rights and Privacy Act (FERPA), that in order to receive federal funding, schools must offer certain rights to parents of students and to students over the age of 18, including the right to inspect and review the student's education records, as defined, and the right to request that the school correct records that are inaccurate or misleading; and must place certain restrictions on the disclosure of any information from a student's education record without written consent from the parent or adult student, except under specified circumstances. (20 U.S.C. Sec. 1232g.)

3) Requires, pursuant to the federal Children's Online Privacy Protection Act (COPPA), that an operator of an internet website or online service directed to a child, as defined, or an operator of an internet website or online service that has actual knowledge that it is collecting PI from a child, to provide notice of what information is being collected and how that information is being used, and to give the parents of the child the opportunity to refuse to permit the operator's further collection of information from the child. (15 U.S.C. Sec. 6502.)

4) Establishes the K-12 Pupil Online Personal Information Protection Act (POPIPA), which prohibits the operator of an internet website, online service, online application, or mobile

application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes, from engaging in specified activities with respect to their site, service, or application, including:

a. Engaging in targeted advertising on the operator's site, service or application, or targeting advertising on any other site, service, application when the targeting of the advertising is based on any information that the operator has acquired because of the use of that operator's site, service, or application.

b. Using information created or gathered by the operator's site, service, or application, to amass a profile about a K-12 student except in furtherance of K-12 purposes.

c. Sell a student's information.

d. Disclose covered information, as defined, except under specified circumstances. (Bus. & Prof. Code § 22584.)

5) Requires, pursuant to POPIPA, that an operator implement reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure; and delete a student's covered information if the school or district requests deletion of data under the control of the school or district. (Bus. & Prof. Code § 22584(d).)

6) Pursuant to the Early Learning Personal Information Protection Act (ELPIPA), extends specified POPIPA protections to children enrolled in preschool or prekindergarten courses of instruction. (Bus. & Prof. Code § 22586.)

7) Prohibits an operator of an internet website, online service, online application, or mobile application directed to minors from marketing or advertising specified products or services that cannot be legally purchased by minors if the operator has actual knowledge that the person to whom they are advertising is a minor; and prohibits an operator who has actual knowledge that a minor is using its website, online service, online application, or mobile application from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the PI of a minor with actual knowledge that the use, disclosure, or compilation is for the purpose of marketing or advertising products or services to that minor for a specified product. (Bus. & Prof. Code § 22580.)

8) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

a. The right to know what personal information (PI) a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI.

b. The right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold.

c. The right to access the specific pieces of information a business has collected about the consumer.

d. The right to delete information that a business has collected from the consumer.

e. The right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in if the consumer is a minor (as exercised by the parent if the minor is under 13, or as exercised by the minor if the minor is between ages 13 and 16).

f. The right to equal service and price, despite exercising any of these rights. (Civ. Code § 1798.100 *et seq.*)

9) Pursuant to the CCPA, permits any consumer whose non-encrypted and non-redacted PI is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to institute a civil action to recover specified damages, injunctive or declaratory relief, and any other relief the court deems proper. (Civ. Code § 1798.150.)

10) Requires a business providing proctoring services in an educational setting to collect, use, retain, and disclose only the personal information strictly necessary to provide those services, except as necessary to do any of the following:

a. To comply with federal, state, or local law.

b. To comply with a court order or subpoena.

c. To comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local agency authorized by law to conduct that inquiry or investigation, or authorized to serve a subpoena or summons, as applicable.

d. To cooperate with a law enforcement agency concerning conduct or activity that the business reasonably and in good faith believes to violate federal, state, or local law.

e. To cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at imminent risk of death or serious physical injury, provided that all of the following are met:

i. The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

ii. The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

iii. The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

f. To exercise or defend a legal claim. (Bus. & Prof. Code § 22588.)

THIS BILL:

1) Defines the following terms:

   a. "End-to-end encryption" or "E2EE" to mean a security method where data is encrypted on the sender's device and remains encrypted until it reaches the intended recipient's device and is unreadable by any other party, including the business providing proctoring services.

   b. "Local educational agency" to mean a school district, county office of education, or charter school.

2) Requires a business providing proctoring services to a local educational agency for classroom- or course-based exams in an educational setting to use end-to-end encryption to provide those services.

COMMENTS:

1) **Author's statement.** According to the author:

   In the wake of the COVID-19 pandemic, schools across California rapidly adopted online learning platforms and virtual assessments both inside and outside the classroom. Due to their flexibility and efficiency, these digital tools remain widely used, transforming our K–12 education system. Unfortunately, some third-party proctoring companies have collected sensitive student data far beyond what is necessary to administer exams, including biometric information, browsing history, and recordings from students' homes. This excessive data collection raises serious privacy and security concerns.

   Existing laws such as the California Consumer Privacy Act and the Family Educational Rights and Privacy Act provide important privacy protections. However, as technology evolves and becomes more deeply embedded in education, additional safeguards are necessary to ensure those protections remain meaningful in practice.

   SB 930 strengthens existing law by requiring proctoring companies to implement end-to-end encryption for online assessments. This ensures sensitive student data is protected from unauthorized access, reduces the risk of breaches, and reinforces the principle that students should be able to pursue their education without sacrificing their privacy. Protecting student data is a matter of educational equity, and as technology advances, so must California's commitment to keeping our youth safe.

2) **Background.** *End-to-end encryption.* Encryption is the process of transforming readable information into an unreadable form using an encryption algorithm – a set of rules or calculations – and a cryptographic key. End-to-end encryption, or E2EE, is a method of securing communications so that only the sender and intended recipient can read the content. When information is sent, it is encrypted on the sender's device and remains encrypted while it travels through servers, networks, service providers, and any other intermediaries. Once the information reaches the intended recipient's device, it is decrypted using the appropriate cryptographic key. As a result, intermediaries generally cannot access or interpret the content of the communication.

Student privacy. The privacy of students is afforded special protection under both state and federal law. The Family Educational Rights and Privacy Act (FERPA) provides that in order to receive federal funding, schools must offer certain rights to parents of students and to students over the age of 18, including the right to inspect and review the student's education records and the right to request that the school correct records that are inaccurate or misleading. FERPA also predicates the provision of federal funds to a school on compliance with certain restrictions on disclosing any information from a student's education record without written consent from the parent or adult student, except under specified circumstances. FERPA defines "education records" to include records, files, documents and other materials which contain information directly related to a student and are maintained by an educational agency or institution, or by a person acting for such agency or institution.

California law provides similar protections for education records, and expands on these protections by specifically addressing privacy in the context of educational technology. In 2014, the K-12 Pupil Online Personal Information Protection Act (POPIPA), was established following the passage of SB 1177 (Steinberg). POPIPA regulates operators of internet websites, online services, online applications, and mobile applications with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. In 2016, AB 2799 (Chau), expanded these protections to children enrolled in preschool or prekindergarten. Under these laws, operators are prohibited from knowingly targeting advertising via the operator's service, or targeted advertising via another site or service when the targeting is based upon information that the operator acquired via the operator's service; using information created or gathered by the operator's service to amass a profile about a K-12 student except in furtherance of K-12 school purposes; selling a student's information; or disclosing certain types of personally identifiable information, except under specified circumstances.

SB 1172 (Pan, 2022) expanded on FERPA and POPIPA by requiring businesses providing proctoring services in educational settings to collect, use, retain, and disclose only the PI strictly necessary to provide those services. Consumers whose PI is collected, used, retained, or disclosed in violation of the bill are able to bring civil actions against proctoring service providers.

Proctoring services. During the COVID-19 pandemic, academic institutions turned to online proctoring services to monitor students taking online exams. These services sought to deter cheating, uphold academic integrity, and support students through identity verification, video and audio monitoring, student device controls, live remote proctoring, and automated proctoring through artificial intelligence. As the prevalence of online proctoring services has increased, students have raised concerns regarding the breadth of personal information collected. Electronic Frontier Foundation and Privacy Rights Clearinghouse, co-sponsors of SB 1172, describe the issue in a letter of support for that measure:

> California's students [face] serious privacy risks from remote proctoring software. Remote proctoring companies collect biometric data such as facial recognition templates and fingerprints, citizenship data and medical information, browsing history, and video and audio of a user's surroundings. This information is not necessary to administer an examination, and needlessly places students' privacy at risk . . . The use of proctoring software has risen 500 percent over the course of the pandemic.

A 2020 Consumer Reports article offers further explanation:

> An analysis of Proctortrack software leaked in a databreach this fall suggests that the company ignored basic data security practices. That raises the possibility that private, sensitive information on students was leaked. In addition, security and legal experts worry that colleges don't do enough to ensure online proctoring companies safeguard the personal data they collect.
>
> Videos of students taking tests may have been accessible to unauthorized employees at Proctortrack, along with facial recognition data, contact information, digital copies of ID cards, and more, according to Patrick Jackson, the chief technology officer for the cybersecurity firm Disconnect, who analyzed Proctortrack's leaked source code on behalf of Consumer Reports. After the software leaked, the information could have been accessed by criminals, as well.[1]

3) **What this bill would do**. SB 930 builds on the framework established by SB 1172 by additionally requiring businesses providing proctoring services to local educational agencies for classroom- or course-based exams to use end-to-end encryption to provide those services. The bill's definition of "end-to-end encryption" specifically requires that data be unreadable by the business providing proctoring services. Oakland Privacy, writing in support of the measure, explains the bill's importance:

> Now that education has largely, although not entirely, returned to in-person pedagogy, new problems are emerging. Among them are several well-publicized and large-scale hacks of educational software companies including Powerschool[2], and Illuminate[3]. What these hacks reveal is that despite standing California laws designed to minimize the amount of personal information collected by ed tech companies (SOPIPA et al), the companies seem to have a lot of student information on hand, and significant vulnerability to cybersecurity incidents.
>
> By mandating end to end encryption, Senate Bill 930 seeks to eliminate the risks of company non-compliance to students in the event of hacking or interception by making the transmittals of data points from proctoring software unreadable by the software's manufacturer, and presumably, all others.

ARGUMENTS IN SUPPORT:

The California Teachers Association writes:

> SB 930 takes an important privacy by design approach by requiring end-to-end encryption for online assessments. By ensuring that student data is encrypted on the student's device and

---

[1] Thomas Germain, "Poor Security at Online Proctoring Company May Have Put Student Data at Risk," *Consumer Reports*, Dec. 10, 2020, https://www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk-a8711230545/

[2] Kevin Collier, "Children's data hacked after school software firm missed basic security step, internal report says," *NBC News,* (Jan. 31, 2025), https://www.nbcnews.com/tech/security/powerschool-hack-data-breach-protect-student-school-teacher-safe-rcna189029.

[3] Insurance Journal, "California Gets $3.2M Settlement From Software Company for Breached Student Data," (Nov. 10, 2025), https://www.insurancejournal.com/news/west/2025/11/10/846901.htm.

> remains inaccessible to proctoring vendors, the bill builds protection directly into the system and reduces the risk of misuse or breach from the outset.

Proctoring service provider Proctorio writes:

> Proctorio supports SB 930 because it establishes a clear and uniform baseline for protecting student data across the proctoring industry. We believe that strong privacy protections and educational innovation must go hand in hand, and that clear statutory standards benefit students, families, educators, and providers alike.

The Alameda County Office of Education writes:

> We feel that the requirements of this bill are reasonable and reflect best practices for ensuring students' data privacy.

REGISTERED SUPPORT / OPPOSITION:

Support

First Day Foundation (Co-Sponsor)
Los Amigos De LA Comunidad, INC. (Co-Sponsor)
Alameda County Office of Education
California Catholic Conference
California Teachers Association
Immigrants Rising
Los Angeles County Office of Education
Oakland Privacy
Proctorio, INC.
Wonder Wood Ranch

Opposition

None on file.

Analysis Prepared by: Slater Sharp / P. & C.P. / (916) 319-2200