Date of Hearing: July 1, 2026

ASSEMBLY COMMITTEE ON EDUCATION
Darshana R. Patel, Chair
SB 930 (Reyes) – As Amended March 25, 2026

SENATE VOTE: 37-0

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

[Note: This bill was double referred to the Assembly Committee on Privacy and Consumer Protection and was heard by that Committee as it relates to issues under its jurisdiction.]

SUMMARY: Requires a business providing exam proctoring services to a local educational agency (LEA) to use end-to-end encryption (E2EE), subject to existing requirements for compliance with law enforcement activities. Specifically, **this bill**:

1) Defines the following to mean:

    a) Proctoring services includes, but is not limited to, services offered by a business to observe, monitor, or administer an exam;

    b) E2EE means 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; and

    c) LEA means a school district, county office of education, or charter school.

2) Requires a business that is proctoring classroom- or course-based exams in a kindergarten through 12th grade setting to use E2EE encryption in their proctoring services, such that only the intended recipient, and not the business providing proctoring services, may access the data.

3) Requires the provisions of this bill to be consistent with the California Privacy Rights Act of 2020, enacted by Proposition 24 (2020).

EXISTING LAW:

1) Establishes the Student Test Taker Privacy Protection Act. 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; and

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. (Business and Professions Code (BPC) 22588)

2) Establishes the California Consumer Privacy Act, 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. Specifies that compliance obligations in respecting these rights are the responsibility of businesses. Exempts government entities or nonprofits from compliance. (Civil Code (CIV) 1798.100)

3) Establishes the Children's Online Privacy Protection Act (COPPA). Requires an operator of a website or online service that is directed to a child, or knowingly collecting personal information from a child, to provide notice of the information that is collected and how it is used, and to give parents the opportunity to refuse further information collection from the child. (15 U.S.C. Sec. 6502.)

4) Establishes the K-12 Pupil Online Personal Information Protection Act. Prohibits the operator of a 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, including:

a) Engaging in targeted advertising 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 to amass a profile about a K-12 student except in furtherance of K-12 purposes;

c) Sell a student's information; and

d) Disclose covered information, as defined, except under specified circumstances. (BPC 22584)

FISCAL EFFECT: This bill has been keyed non-fiscal by the Office of Legislative Counsel.

COMMENTS:

Need for the bill. 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.

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."

Online proctoring. The use of computer-based test-taking for K12 students has been rising in recent years, especially in the wake of the COVID-19 pandemic. Many state testing requirement are now met through online platforms, including the California Assessment of Student Performance and Progress (CAASPP).

Importantly, SB 930 defines "proctoring" to include any business that observes, monitors, or administers an exam. This is a broad definition that likely captures the majority of digital test taking in California.

What is end to end encryption? E2EE ensures that data that is transmitted or stored digitally can only be viewed by the sender and the intended recipient. According to the Electronic Frontiers Foundation:

> If used correctly, end-to-end encryption can help protect the contents of your messages, text, and files from being read by anyone except their intended recipients. End-to-end encryption tools make messages unreadable to eavesdroppers on the network, as well as to service providers themselves. They can also prove a message came from a specific person and was not altered.
>
> Once complicated to set up, end-to-end encryption tools are far more usable than they used to be… Here's how encryption works when sending a secret message:
>
> 1. A clearly readable message is first encrypted into a scrambled message that is incomprehensible to anyone looking at it ("hello mum" turns into "OhsieW5ge+osh1aehah6").
>
> 2. The encrypted message is sent over the internet, where, if they're watching, eavesdroppers would only see the scrambled message ("OhsieW5ge+osh1aehah6").
>
> 3. When it arrives at its destination, the intended recipient, and only the intended recipient, has some way of decrypting it back into the original message ("OhsieW5ge+osh1aehah6" is turned back into "hello mum").

In the context of student test taking, the sender of the data is the student and the intended recipient is presumably a school administrator. Ensuring that all relevant school employees are able to access student results in a timely and efficient manner will be an important aspect of SB 930 implementation.

E2EE can be accomplished through multiple methods, such as Advanced Encryption Standard (AES) and Post Quantum Standard (PQS), which each offer different levels of protection. SB 930 does not specify which form of data encryption must be applied to student assessments, which may allow the bill to remain relevant as new forms of encryption become available. However, given that some encryption methods are less secure than others, future legislation may wish to consider requiring stricter encryption standards to protect student data.

Data privacy concerns in online education. Recent and ongoing lawsuits demonstrate the security concerns online education services pose to students:

- In 2025, parents of four California students sued i-Ready (and parent company Curriculum Associates) for allegedly collecting and sharing student information without consent (*M.C. v. Curriculum Associates*). i-Ready is accused of selling student names, ID numbers, grade levels, responses to academic questions, and IP addresses to third-party vendors, including Google. The case is currently ongoing.

- In 2026, PowerSchool (parent company of Naviance) agreed to a $17.25 million settlement after a class action lawsuit accused them of transmitting private communications between students and teachers, along with student names, ID numbers, graduation years, and demographic information, to the companies Google, Microsoft, and Heap (*Q.J. v. PowerSchool Holdings LLC, et a.l*). Attorneys in the case likened PowerSchool's activities to wiretapping and eavesdropping.

- In 2025, Illuminate Education agreed to a $5.1 million settlement with California, Connecticut, and New York after misrepresenting its privacy practices and failing to protect student data. Under the agreement, Illuminate must also implement a robust data security system, including encryption practices. Another lawsuit, filed in May 2026, alleges that Illuminate collects student medical information, which was inadvertently released in a recent data breach (*J.M. v. Illuminate Education).*

- In 2020, a complaint was filed with the Department of Justice regarding data malpractice from exam proctoring companies (*EPIC Complaint in Online Test Proctoring Companies*). For example, the company ProctorU was accused of maintaining a "Hall of Fame" compilation video of students accused of cheating, and was criticized by the University of California Santa Barbara Faculty Association for collecting and sharing student information, including social security numbers, behavioral characteristics, faceprints and retina scans, IP addresses and search history, medical information, and employment information, among other items.

In these examples, providers of online education services released student information to outside entities. Under the E2EE required by SB 930, online proctoring companies would be unable to view or access student information, which could eliminate their ability to share it.

However, these examples illustrate that data breaches go beyond K12 proctoring services. Future legislation may wish to consider extending the E2EE requirements to all online education services, both for the K12 and higher education spaces.

Existing protections for students online are difficult to enforce. In 2014, as digital education tools began to proliferate, SB 1177 (Steinberg, Chapter 839, Statutes of 2014) established POPIPA. POPIPA restricts the use and disclosure of the personally identifiable information or materials of K-12 students. Under POPIPA, businesses that operate online websites, services, or applications (including mobile applications) that are primarily designed or used for K12 purposes cannot use or sell a student's personal information.

Despite passing POPIPA, data breaches and lawsuits revealed that education technology companies continued to collect and share student information (see above examples). In response, the Legislature passed the Student Test Taker Privacy Protection Act (SB 1172 (Pan), Chapter 720, Statues of 2022). The Act prohibited proctoring companies from collecting, using, retaining, and disclosing any personal information from test takers beyond what was strictly necessary to provide the proctoring services. The statute also includes some exemptions, such as complying with orders from law enforcement agencies or in emergency settings.

However, the enforcement mechanisms available under POPIPA and the Test Taker Protection Act are primarily lawsuits, which can be filed only after the harm has occurred. Under the encryption requirements in SB 930 companies would likely be unable to access student data at all, thereby acting as a preventative method rather than a reactive one. For this reason, supporters of SB 930 argue that it is a needed supplement to existing student privacy laws.

Arguments in support. According to the Los Angelos County Office of Education, "As educational institutions continue to expand the use of online and hybrid testing environments, protecting student information has become increasingly important. Students routinely provide sensitive personal information through digital assessment platforms, making strong cybersecurity safeguards essential to maintaining trust, privacy, and compliance with state data protection laws.

By requiring end-to-end encryption for online test proctoring services, SB 930 strengthens protections for student data and reduces the risk of unauthorized access to personal information during assessments. Ensuring that information remains encrypted from the sender's device until it reaches the intended recipient provides an important safeguard against data breaches and unauthorized disclosure.

The bill promotes safer digital learning environments for both students and staff by establishing a clear security standard for vendors providing assessment-related services. While implementation may require some vendors to enhance their existing security capabilities, the requirement aligns with widely recognized industry best practices and supports local educational agencies in meeting evolving expectations related to student privacy and cybersecurity.

As technology continues to play a greater role in teaching, learning, and assessment, strengthening protections for student data is essential to ensuring secure and effective educational environments."

Arguments in Support. According to the First Day Foundation, "California has long been a national leader in privacy protection, from the California Consumer Privacy Act to the California Privacy Rights Act. SB 930 continues this legacy by extending strong protections to our K-12 students, who should not have to surrender intimate details about their home life, their appearance, their disabilities, or their online activity to a private company simply to take an exam. SB 930 also protects school districts from the legal and financial risks associated with third-party data breaches. This is a common-sense safeguard that benefits students, families, and schools alike."

Recommended Committee Amendments. Staff recommends that the bill be amended as follows:

1) Include an implementation date of July 1, 2027.

Related legislation. SB 1172 (Pan), Chapter 720, Statutes of 2022, created the Pupil Test Taker Privacy Protection Act, which restricts the personal information that a business providing educational proctoring services can collect, use, retain, and disclose.

AB 375 (Chau), Chapter 55, Statutes of 2018, established the California Consumer Privacy Act, which grants consumers certain rights regarding their personal information.

SB 1177 (Steinberg), Chapter 839, Statutes of 2014, established POPIPA to restrict the use and disclosure of information about K-12 students.

REGISTERED SUPPORT / OPPOSITION:

Support

Alameda County Office of Education
California Teachers Association
First Day Foundation
Immigrants Rising
Los Amigos De LA Comunidad, INC.
Los Angeles County Office of Education
Oakland Privacy
Wonder Wood Ranch

Opposition

None on file

Analysis Prepared by: Sarah Cate Hawthorne / ED. / (916) 319-2087