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

SB 930 (Reyes)
Version: March 25, 2026
Hearing Date: April 6, 2026
Fiscal: No
Urgency: No
BH

SUBJECT

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

DIGEST

This bill requires a business providing proctoring services to a local educational agency, as provided, to use end-to-end encryption, as defined, in providing those services to protect personal information.

EXECUTIVE SUMMARY

Proctoring software collects sensitive information, such as video, audio, and screen data, but most current systems lack robust encryption safeguards. End-to-end encryption (E2EE) ensures that data is encrypted on the student's device and remains protected during transmission and storage, accessible only to authorized school personnel—not to the proctoring vendor itself, or any other party. Current law allows proctoring companies to use the data to provide the necessary proctoring services.

This bill fortifies the Student Test Taker Privacy Protection Act by requiring that businesses providing proctoring services to specified educational institutions use E2EE to provide those services. E2EE is defined as 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.

This bill is sponsored by First Day Foundation and Los Amigos de la Comunidad. The bill is supported by a number of groups, including the Center for Digital Democracy, the Alameda County Office of Education, and Oakland Privacy. No timely opposition has been received by the Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Prohibits a business providing proctoring services in an educational setting from collecting, retaining, using, or disclosing personal information except to the extent necessary to provide those proctoring services, as specified. (Bus. & Prof. Code § 22588(a).)

3) Provides that the above restriction does not prohibit a business from collecting, using, retaining, or disclosing personal information if doing so is necessary for specified purposes, including to comply with federal or state laws or a court order or subpoena. (Bus. & Prof. Code § 22588(b)).

4) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to 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. It does not apply to government entities or nonprofits. (Civ. Code § 1798.100 et seq.)

This bill:

1) Requires a business providing proctoring services to a local educational agency for classroom or course-based exams to use E2EE to provide those proctoring services.

2) Provides the following definitions:
    a) "End-to-end encryption" or "EE2E" 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.
    b) "Local educational agency" means a school district, county office of education, or charter school.

COMMENTS

1. Tests are important

For a student, tests represent a hurdle that must be cleared to advance their academic, professional or personal lives. Test proctors are important as they provide test security, fidelity and data assessment for the testing process. The rise of online testing has

provided students with greater flexibility and access to testing opportunities like never before. Online proctored testing, or remote proctoring, is the practice of monitoring students taking such online exams with software and services. The purpose is to deter cheating, uphold academic integrity, and support students. These goals are accomplished through various methods, including identity verification, video and audio monitoring, locking other functions of a student's computer, live remote proctoring, automated proctoring using AI, or some hybrid model. These services exploded during the COVID-19 pandemic.

Like all technological advances, the benefits come with drawbacks, especially with regard to individuals' privacy. Online exams have exposed significant vulnerabilities in the protection of student personal data.

In response to rising concerns, SB 1172 (Pan, Ch. 720, Stats. 2022) created the Student Test Taker Privacy Protection Act. That law requires a business providing proctoring services in an educational setting to collect, use, retain, and disclose only the personal information strictly necessary to provide that service. However, it provides a series of exemptions from that requirement and does not provide for consumer enforcement.

2. Enhancing student privacy protections

Proctoring software collects sensitive information, such as video, audio, and screen data. Unfortunately, most current proctoring systems lack robust encryption safeguards to protect such sensitive student data. This bill attempts to address that gap by amending the Student Test Taker Privacy Protection Act to require a business providing proctoring services to a local educational agency for classroom or course-based exams to use E2EE to provide those proctoring services.

According to IBM:

> End-to-end encryption (E2EE) is a secure communication process that encrypts data before transferring it to another endpoint. Data stays encrypted in transit and is decrypted on the recipient's device. Messaging apps, SMS, and other communications services rely on E2EE to protect messages from unauthorized access.
>
> End-to-end encryption (E2EE) is widely considered the most private and secure method for communicating over a network.
>
> Similar to other encryption methods, E2EE transforms readable plaintext into unreadable ciphertext by using cryptography. This process helps to mask sensitive information from unauthorized users and ensures that

> only the intended recipients—with the correct decryption key—can access sensitive data.[1]

E2EE ensures that data is encrypted on the student's device and remains protected during transmission and storage. The data is accessible only to authorized school personnel, but not to the proctoring vendor itself.

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.

The Center for Digital Democracy writes in support:

> Privacy is a fundamental right, and for students it is also a matter of data justice. Young people are required to use digital systems that collect highly sensitive information, often without meaningful choice, creating structural risks and imbalances that demand stronger protections.

---

[1] *What is end-to-end encryption (E2EE)?* IBM, https://www.ibm.com/think/topics/end-to-end-encryption [as of March 29, 2026].

Online proctoring technologies highlight these concerns. They collect video, audio, biometric, and behavioral data, yet current safeguards remain inadequate. Students should not have to accept intrusive surveillance in order to participate in their education.

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

This is a necessary step to rebalance power, limit unnecessary data access, and ensure that educational technology respects students' rights in practice.

SUPPORT

First Day Foundation (co-sponsor)
Los Amigos de la Comunidad (co-sponsor)
Alameda County Office of Education
Center for Digital Democracy
Oakland Privacy
Proctorio, Inc.
Wonder Wood Ranch

OPPOSITION

None received

****