SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

SB 1172 (Pan)
Version: February 17, 2022
Hearing Date: April 5, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Privacy Rights Act of 2020: business: proctoring services

DIGEST

This bill restricts the personal information that a business providing educational proctoring services can collect, use, retain, and disclose. The bill provides consumers an enforcement mechanism for any violations thereof.

EXECUTIVE SUMMARY

Online proctored testing, or remote proctoring, is the practice of monitoring students taking 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 have exploded in recent years due in large part to the COVID-19 pandemic. One survey estimates that over half of higher education institutions are using the services with an additional one quarter of them planning to or considering it.

Like all technological advances, the benefits come with drawbacks, especially with regard to individuals' privacy. This bill responds to concerns about what information is being collected by the businesses providing these online proctoring services and what is being done with it. The bill 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.

This bill is sponsored by the Electronic Frontier Foundation and Privacy Rights Clearinghouse. It is supported by a variety of groups, including The Greenlining Institute and ACLU California Action. The bill is opposed by the California Chamber of Commerce and the Civil Justice Association of California.

PROPOSED CHANGES TO THE LAW

Existing federal law:

1) Establishes the Children's Online Privacy Protection Act of 1998 (COPPA), 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.S. § 6501; 16 C.F.R. Part 312.)

2) 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.)

Existing state law:

3) Establishes the Student Online Personal Information Protection Act (SOPIPA) to restrict the use and disclosure of the personally identifiable information or materials of K-12 students. (Bus. & Prof. Code § 22584.)

4) Prohibits an operator of an Internet Web site, online service, online application, or mobile application, as specified, from marketing specified types of products or services to a minor and from knowingly using, disclosing, compiling, or knowingly allowing a 3rd party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising specified types of products or services. It also authorizes minor users to remove, or to request and obtain removal of, content or information publicly posted by the minor, subject to specified conditions and exceptions. (Bus. & Prof. Code § 22580.)

5) Establishes the 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. (Civ. Code § 1798.100 et seq.)

6) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

7) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the following:
    a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;
    b) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and
    c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose. (Civ. Code § 1798.100(a).)

8) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting or selling personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

9) Provides consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer the following:
    a) the categories of personal information that the business collected about the consumer;

b) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
c) the categories of personal information that the business disclosed about the consumer for a business purpose. (Civ. Code § 1798.115.)

10) Provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold and that consumers have the right to opt out of the sale of their personal information. (Civ. Code § 1798.120.)

11) Provides that these provisions do not restrict a business' ability to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information. (Civ. Code § 1798.145(a)(6).)

12) Defines "personal information" as 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. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." (Civ. Code § 1798.140(v)(1).)

13) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as genetic data and the processing of biometric information for the purpose of uniquely identifying a consumer. (Civ. Code § 1798.140(ae).)

14) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

15) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

This bill:

1) Requires, notwithstanding subdivision (a) of Section 1798.100 and paragraph (6) of subdivision (a) of Section 1798.145 of the Civil Code, 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.

2) Authorizes a consumer whose personal information is collected, used, retained, or disclosed in violation of these provisions to bring a civil action against that business and may recover all of the following:
    a) liquidated damages of $1,000 per consumer per incident or actual damages, whichever is greater;
    b) injunctive or declaratory relief; and
    c) reasonable attorney fees and costs, including expert witness fees.

3) Provides that the Legislature finds and declares that this bill furthers the purpose and intent of the California Privacy Rights Act of 2020, enacted by Proposition 24 at the November 3, 2020, statewide election, within the meaning of Section 25 of Proposition 24.

COMMENTS

1. Existing laws protecting students' privacy

The Children's Online Privacy Protection Act of 1998 (COPPA) imposes 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.S. § 6501; 16 C.F.R. Part 312.) COPPA makes it unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Broadly, COPPA requires these operators to do the following:

- provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information;
- obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
- provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;
- not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
- establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. (20 U.S.C. § 1232g; 34 C.F.R. Part 99.) The law applies to all schools that receive certain federal funding. Generally, schools must have written permission from the parent or eligible student in order to release information from a student's

education record. However, FERPA allows schools to disclose those records, without consent, to certain parties or under certain conditions. This includes disclosure to school officials with legitimate educational interests specified officials for audit or evaluation purposes.

The Student Online Personal Information Protection Act (SOPIPA) restricts the use and disclosure of the personally identifiable information or materials of K-12 students. (Bus. & Prof. Code § 22584.) It regulates operators of Internet Web sites, online services, online applications, or mobile applications with actual knowledge that the sites, services, or applications are used primarily for K–12 school purposes and were designed and marketed for K–12 school purposes. It prohibits operators from knowingly engaging in specified activities with respect to their site, service, or application. This includes:

- engaging in targeted advertising when the targeting of the advertising is based upon any information that the operator has acquired because of the use of that operator's site, service, or application;
- use of information, including persistent unique identifiers, 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 school purposes; or
- selling a student's information.

SOPIPA also restricts disclosing the information but provides various exceptions, including where the disclosure is in furtherance of the K–12 purpose of the site, service, or application. Operators are also required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and protect that information from unauthorized access, destruction, use, modification, or disclosure. They must delete a student's information if the school or district requests deletion of data under the control of the school or district.

The California Consumer Privacy Act of 2018 (CCPA) 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. (Civ. Code § 1798.100 et seq.) It places attendant obligations on businesses to respect those rights. In the November 3, 2020 election, voters approved Proposition 24, which established the California Privacy Rights Act of 2020 (CPRA). The CPRA amends the CCPA, limits further amendment, and creates the California Privacy Protection Agency (PPA).

2. Building on existing law

As discussed above, with the expanded use of online proctoring services, have come concerns regarding what information is being collected in connection with those services and what is being done with it.

According to the author:

> Students should not have to surrender their privacy information to third-party software companies simply to take examinations. The exponential rise in online test-taking has led to an increase in personal biometric information that is collected. There are well documented cases of proctoring companies that have collected more than the necessary information to administer tests and have often times held on to that information for long periods of time. The collection of this information seriously compromises the safety of young students in the case of data breaches or even the egregious practice of selling or sharing personal consumer information. Currently, the California Consumer Privacy Act (CCPA) and the Federal Family Education Rights and Privacy Act (FERPA), fall short of protecting students due to loopholes that allow proctoring companies to distance their accountability to students by emphasizing their primary relationship with the school and not the consumer or students. Senate Bill 1172 is a sensible measure that protects our students by limiting data collection, strengthening privacy protections, and increasing accountability by creating an enforcement mechanism to empower student test-takers who have been harmed.

The co-sponsors of the bill, the Electronic Frontier Foundation and Privacy Rights Clearinghouse, assert:

> S.B. 1172 addresses a growing concern for California's students, who 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. Proctoring companies should not collect the information in the first place, which is why we support placing strict data minimization requirements on them.
>
> The use of proctoring software has risen 500 percent over the course of the pandemic. Apart from the amount of data this software collects, many questions have been raised about its effectiveness at correctly identifying or preventing cheating. For example, more than one-third of California Bar examinees were flagged as cheating—on its face, a ridiculous assertion. California's state government has already recognized the problem that the STTPPA would address. In late 2020, the California Supreme Court directed the California State Bar to prepare a timetable for destruction of all bar examinees' personally identifiable information retained by the remote proctoring company (ExamSoft). The court

> recognized that some data collection was unrelated to the administration of the bar, and that unnecessary retention of sensitive personally identifiable information increases the risk of unintentional disclosure. The STTPPA would enshrine this sort of requirement in law.

The concerns are heightened in not uncommon situations where students are required to use these services in order to take a required test or are given less than ideal alternatives. Although many proctoring companies declare that they only begin monitoring a student and collecting their information after notice and consent is provided, such consent is arguably hollow when there are not viable alternatives and when there is clear pressure to accept such conditions from their educational institution.

Supporters of the bill point to instances that they feel validate these concerns:

> College and high school students across the country have objected to online proctoring programs from Proctortrack and a number of other companies, such as Proctorio, ProctorU, Honorlock, and Respondus Monitor, which all perform surveillance on students while they take tests. The students say the systems are intrusive and make remote exams very stressful.
>
> Now, there's evidence of another problem. An analysis of Proctortrack software leaked in a data breach 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]

Various lawsuits have also risen up to try and combat the more problematic practices. For instance, the Electronic Privacy Information Center (EPIC) filed a complaint against five online test-proctoring services: Respondus, ProctorU, Proctorio, Examity, and Honorlock:

---

[1] Thomas Germain, *Poor Security at Online Proctoring Company May Have Put Student Data at Risk* (December 10, 2020) Consumer Reports, https://www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk-a8711230545/. All internet citations are current as of March 22, 2022.

> EPIC claims that the firms violate the privacy rights of students.
>
> The five companies sell software designed to prevent cheating in online tests and exams. Some are designed to track applications that are running on test-takers' computers or restrict access to certain programs during the testing period. Others track students' activity during the test via their webcams and microphones and flag potentially suspicious behavior to their instructor, using either algorithms or live monitoring. In some cases, test-takers need to show a proctor their surroundings and verify their identity with personal information before the test can begin.
>
> These methods — the collection of personal information and the use of "secret algorithms" — amount to "unfair and deceptive trade practices," EPIC argues.
>
> "Respondents' collection of sensitive personal information, including biometric data, is unjustified, excessive, and harmful to students who have no meaningful opportunity to opt out of such systems," the complaint further reads. "Forcibly collecting personal information from test-takers, including sensitive biometric data, is inherently invasive."
>
> The use of remote test-proctoring services has skyrocketed with this year's rise in online instruction at all grade levels. So, too, has scrutiny on its providers. Proctorio (one of EPIC's targets, which over 400 universities use) came under fire earlier this year for its suite of "machine learning and advanced facial detection technologies," which monitor the position of a student's head while they take their test and flags possible signs of cheating. Critics called the service discriminatory, anxiety-provoking, and an invasion of privacy. Thousands of students have signed petitions and open letters calling on their schools to get rid of the service.[2]

In order to respond to these concerns, this bill limits a business providing proctoring services in an educational setting to collecting, using, retaining, and disclosing only that personal information which is strictly necessary to provide those services. This data minimization requirement ensures that there is not an unnecessary intrusion of privacy at the point of collection. It also limits what can be done with the information once collected. To ensure that this information is not being used to build profiles on students or being sold to data brokers and others, disclosure is limited to only what is necessary to accomplish the relevant proctoring purposes. The provision also ensures that unnecessary personal information is not retained and therefore available should a

[2] Monica Chin, *Privacy group files complaint against five online test-proctoring services* (December 9, 2020) The Verge, https://www.theverge.com/2020/12/9/22166023/epic-proctorio-examity-privacy-online-testing-school-lawsuit-proctoring.

breach occur. This is particularly critical given the scope. Proctorio, a leading proctoring company, reports that in 2020, at the height of the COVID-19 pandemic, it proctored over 20,000,000 exams.[3] Examsoft, the company that provides proctoring services in connection with the California bar exam, reports that it has proctored over 90 million tests.[4] Highlighting the real world risk, ProctorU confirmed that in July 2020, one of its databases was breached resulting in the leak of approximately 444,000 records. This included full names, emails, addresses, hashed passwords, and other information. The company indicated that the records were from 2014, therefore, with stricter retention limits, these records would not have even been available.

This bill protects students and their schools from unnecessary intrusions on privacy and security risks. This bill fills in some of the gaps of the other laws discussed above in the context of online proctoring services. For instance, COPPA applies only to young children, and advocates argue it does not limit the information a service may collect once the service provides notice of the information being collected and obtains verifiable parental consent. SOPIPA applies only to K-12 students and, supporters assert, it does not limit the information that can be collected by proctoring services to what is strictly necessary for proctoring. While FERPA should generally protect data collected in educational settings, it does not limit what schools can collect, and there are concerns that information is still being retained and otherwise used/disclosed by proctoring businesses. It also builds on the protections in the CCPA/CPRA by affirmatively requiring data minimization for all information collected in connection with proctoring services and strict limitations on what can be done with it.

Importantly, unlike these other laws, this bill provides consumers a strong enforcement mechanism should their information be collected, used, retained, or disclosed in violation of the bill's provisions. Consumers can seek statutory damages of $1000 per incident or actual damages; injunctive or declaratory relief; and reasonable attorneys' fees and costs. However, those in opposition object to the inclusion of this enforcement mechanism. The Civil Justice Association of California argues:

> What SB 1172 seeks to do is add expanded liability for those providing proctoring services in conflict to the voter approved limited action under the CPRA. Singling out specific industries or services to add additional liability does not align with the CPRA's goal of providing uniformity to how consumer data is treated.

A coalition in support, including the Center for Digital Democracy and Common Sense, disagrees and stresses the need for the bill: "It's clear that current law does not offer enough protection to students subject to remote proctoring. That is why we need

[3] Proctorio web site, *History*, https://proctorio.com/about/history.
[4] Examsoft web site, *About*, https://examsoft.com/about-examsoft/.

stronger protections for Californians. We also need to give them tools to fight back against irresponsible companies."

3. Furthering the purpose and intent of the CPRA

Section 25 of the CPRA, passed by voters in November 2020, requires any amendments thereto to be "consistent with and further the purpose and intent of this act as set forth in Section 3." Section 3 declares that "it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy." It then lays out a series of guiding principles. These include various consumer rights such as:

- consumers should know who is collecting their personal information;
- consumers should have control over how their personal information is used; and
- consumers should benefit from businesses' use of their personal information.

Section 3 also includes a series of responsibilities that businesses should have. These include:

- businesses should specifically and clearly inform consumers about how they use personal information; and
- businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes.

The section also lays out various guiding principles about how the law should be implemented.

Writing in opposition, the California Chamber of Commerce asserts that the bill does not align with the CPRA's intent:

> The underlying goal of SB 1172 appears to be to introduce a new private right of action around the collection, use, retention, and disclosure of personal information by businesses offering proctoring services. This runs contrary to the voters' intent when enacting a comprehensive, industry- and technology- neutral privacy law that treats all personal information and sensitive personal information in a uniform matter, subject to a limited private right of action.

This bill bolsters protections for students in connection with online proctoring services and allows them to enforce these rights. Just as the CPRA itself provides varying degrees of protection depending on the sensitivity of information, this bill bolsters protections that are catered to the unique nuances of proctoring services in the educational setting. Therefore, the bill arguably furthers the purposes and intent of the CPRA to protect consumers' privacy rights.

SUPPORT

Electronic Frontier Foundation (co-sponsor)
Privacy Rights Clearinghouse (co-sponsor)
ACLU California Action
California Medical Association
Center for Digital Democracy
Citizens Privacy Coalition of Santa Clara County
Common Sense
Consumer Action
Consumer Reports
Electronic Privacy Information Center
Fairplay
Fight for the Future
Media Alliance
Oakland Privacy
The Greenlining Institute

OPPOSITION

California Chamber of Commerce
Civil Justice Association of California

RELATED LEGISLATION

Pending Legislation:

SB 746 (Skinner, 2022) amends the CCPA to require businesses to disclose whether they use the personal information of consumers for political purposes, as defined, to consumers, upon request, and annually to the Attorney General or the PPA, as specified. This bill is currently awaiting referral in the Assembly.

SB 1454 (Archuleta, 2022) removes the sunset on the exemption from certain provisions of the CCPA of personal information reflecting a communication or a transaction between a business and a company, partnership, sole proprietorship, nonprofit, or government agency that occurs solely within the context of the business conducting due diligence or providing or receiving a product or service. It also makes permanent the exemption for personal information that is collected and used by a business solely within the context of having an emergency contact on file, administering specified benefits, or a person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business. This bill is currently in this Committee.

AB 2871 (Low, 2022) is identical to SB 1454. This bill is currently awaiting referral in the Assembly.

AB 2891 (Low, 2022) is substantially similar to SB 1454 and AB 2871, but extends, rather than removes, the sunset to January 1, 2026. This bill is currently awaiting referral in the Assembly.

Prior Legislation:

AB 335 (Boerner Horvath, Ch. 700, Stats. 2021) exempted from the California Consumer Privacy Act's right to opt out certain information related to vessels that is retained or shared between a vessel dealer and the vessel's manufacturer, if the information is shared in connection with a vessel repair covered by a vessel warranty or a recall, as specified.

AB 375 (Chau, Ch. 55, Stats. 2018) established the CCPA.

SB 1177 (Steinberg, Ch. 839, Stats. 2014) established SOPIPA.

****