Date of Hearing: June 14, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
SB 1172 (Pan) – As Introduced February 17, 2022

SENATE VOTE: 27-9

SUBJECT: California Privacy Rights Act of 2020: business: proctoring services

SUMMARY: This bill would amend the California Privacy Rights Act of 2020 (CPRA) to require a business providing proctoring services in an educational setting to collect, use, retain, and disclose only the personal information (PI) strictly necessary to provide that service. Specifically, **this bill would**:

1) Require that a business providing proctoring services in an educational setting collect, use, retain, and disclose only the PI strictly necessary to provide that service.

2) Provide that a consumer whose PI is collected, used, retained, or disclosed in violation of 1), above, may bring a civil action against that business and may recover all of the following:

    - Liquidated damages of $1,000 per consumer per incident or actual damages, whichever is greater.

    - Injunctive or declaratory relief.

    - Reasonable attorney fees and costs, including expert witness fees.

3) Find and declare, on behalf of the Legislature, that the provisions of the bill further the purpose and intent of the CPRA.

EXISTING LAW:

1) 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.)

2) 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.)

3) Establishes the Student Online Personal Information Protection Act (SOPIPA), 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:

- 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.

- 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.

- Sell a student's information.

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

4) Requires, pursuant to SOPIPA, that an operator specified in 3), above, 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 Sec. 22584(d).)

5) Pursuant to the Early Learning Personal Information Protection Act (ELPIPA), extends the protections provided in 3) and 4), above, to children enrolled in preschool or prekindergarten courses of instruction. (Bus. & Prof. Code Sec. 22586.)

6) 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 Sec. 22580.)

7) 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:

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

- 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.

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

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

- 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).

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

8) 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 Sec. 1798.150.)

FISCAL EFFECT: According to the Senate Appropriations Committee, "[u]nknown, significant cost pressures, potentially in the hundreds of thousands of dollars, possibly in the low millions, for court workload [because courts] will be responsible for adjudicating violations of the provisions proposed by this bill (Trial Court Trust Fund, General Fund [])."

COMMENTS:

1) **Purpose of this bill**: This bill seeks to protect the privacy of students by restricting the collection, retention, use, and disclosure of PI by businesses operating proctoring services in educational settings to that which is strictly necessary to provide the proctoring service. This bill is co-sponsored by Electronic Frontier Foundation and Privacy Rights Clearinghouse.

2) **Author's statement**: According to the author:

> Students should not have to surrender their privacy information to third-party software companies simply to take examinations. Unfortunately, young people across California are required to use privacy-invasive remote proctoring software when testing remotely. SB 1172, the Student Test-Takers Privacy Protection Act, strengthens protections for Californians using remote proctoring software for tests by requiring data minimization and allowing harmed users of remote proctoring software to sue companies that do not meet these standards.
>
> [CCPA] needs to expand protections as educational technology evolves. The consequential risk with the collection of an abundance of personally identifiable information is data breaches. It is not necessary for proctoring companies to have MORE student personal data than is necessary for a student to take an exam. If companies didn't have it, then we would not be seeing lawsuits and complaints rise across the country [].
>
> The Test Taker Privacy Protection Act directs proctoring companies to create reasonable data minimization and collection practices. In the event data is collected beyond what

was required, test takers have the opportunity to take the proctoring company to court to receive damages. This allows the courts to decide, narrowly and thoughtfully, what data is required to collect for proctoring services, and how long it should be held. It's a simple bill that should give the people harmed – test takers – the opportunity to move the needle forward for protecting their data and privacy.

3) **Proctoring services**: With the rise in remote learning accelerated by the COVID-19 pandemic, the use of online proctoring services to monitor students while taking online exams has exploded. These services are generally employed in an effort to deter cheating, uphold academic integrity, and support students through methods including identity verification, video and audio monitoring, locking other functions of student devices, live remote proctoring, and automated proctoring through artificial intelligence. One survey estimates that over half of higher education institutions are using these proctoring services, with an additional one quarter planning to or considering their use.

With the increasing prevalence of online proctoring services, California students have raised concerns regarding the breadth of PI collected in the process of monitoring test taking, and precisely what is being done with that information. As the Electronic Frontier Foundation and Privacy Rights Clearinghouse, co-sponsors of this bill, explain:

> 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 [this bill] 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. [This bill] would enshrine this sort of requirement in law.

Validating the risk of unintentional disclosure, in July 2020, ProctorU, a proctoring service in opposition to this bill, confirmed a breach of one of its databases resulting in the leak of approximately 444,000 records, including full names, email addresses, home addresses, hashed passwords, and various other data. A 2020 article in Consumer Reports further supports the claims of the sponsors:

> 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]

This bill seeks to minimize the risk of compromise of sensitive student information and protect the privacy of test-takers by requiring that proctoring services minimize the PI the collect, use, retain, and disclose to that which is strictly necessary to provide the proctoring service.

4) **Student privacy rights**: The privacy of students is generally afforded special protection under both state and federal law. Federally, education records are protected by FERPA. (20 U.S.C. Sec. 1232g.) 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 the disclosure of 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" broadly, 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, this Legislature passed SB 1177 (Steinberg, Ch. 839, Stats. 2014), which established SOPIPA. SOPIPA specifically regulates the practices of 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, as defined. (Bus. & Prof. Code Sec. 22584.) In 2016, this Legislature passed AB 2799 (Chau, Ch. 620, Stats. 2016), which expanded the same protections to children enrolled in preschool or prekindergarten. (Bus. & Prof. Code Sec. 22586.)

Pursuant to SOPIPA, operators of these services are prohibited from knowingly engaging in specified practices, including: engaging in targeted 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

---

[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/ [as of Jun. 12, 2022].

school purposes; selling a student's information; or disclosing certain types of personally identifiable information, except under specified circumstances. These circumstances include: in furtherance of K-12 purposes provided the information is only further disclosed to allow or improve operability and functionality within the student's classroom or school; to ensure legal and regulatory compliance; to respond to or participate in judicial process; to protect the safety of users or others or security of the site; or to a service provider, as specified.

In addition to these protections specific to educational contexts, California law also provides general protections for PI collected by businesses. In 2018, California enacted landmark privacy legislation, the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), giving consumers certain rights regarding their PI, including: (1) the right to know what PI is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age. (Civ. Code Sec. 1798.100, et seq.) In 2020, California voters passed Proposition 24, which established certain new consumer privacy rights, including the right to opt-in to limiting the use and disclosure of so-called "sensitive personal information" to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer that requests those goods or services. (Civ. Code Sec. 1798.121.) Proposition 24 also established the California Privacy Protection Agency, and renamed the CCPA to the CPRA.

This bill would expand on existing laws protecting the PI of students by specifically prohibiting a proctoring service operating in an educational setting from collecting, retaining, using, or disclosing any PI that is not strictly necessary to provide the proctoring service, and would provide a private right of action to facilitate robust enforcement.

5) **Bill would provide additional protection for student PI in the context of proctoring services by imposing strict data minimization requirements**: Despite these various statutory schemes protecting student PI, proponents of this bill argue there are still loopholes and blind spots that leave student PI under-protected in the context of proctoring services. For instance, SOPIPA only applies in circumstances in which the service is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. This construction neglects the use of proctoring services in higher education, and may even absolve proctoring services of liability under SOPIPA so long as they can mount a legitimate claim that the service is not used *primarily* for K-12 purposes or was not *designed* for K-12 school purposes (e.g. the service is used to similar extents for both K-12 and higher education purposes).

   Additionally, while FERPA places constraints on the disclosure of student education records, it does not limit the collection of student PI in any way, and even permits disclosure in various circumstances. This means that complete compliance with the provisions of FERPA may still leave vast amounts of student PI vulnerable to data breach should such information be collected in excess of what is necessary to provide a given educational service. The CCPA/CPRA provides the right to opt-out of the sale of PI (or in the case of those under 16 years of age, opt-in), but again does not limit collection. Proponents of this bill also argue that these laws lack sufficient enforcement mechanisms to incentivize accountability.

   This bill seeks to resolve these alleged shortcomings in existing law by requiring a business providing proctoring services in an educational setting to collect, use, retain, and disclose

only the PI *strictly necessary* to provide that service. To enforce this data minimization requirement, the bill provides that a consumer whose PI is collected, used, retained, or disclosed in violation of that requirement may bring a civil action against that business and may recover all of the following: liquidated damages of $1,000 per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; and reasonably attorney fees and costs, including expert witness fees.

Given the particular sensitivity of the context in which proctoring services are employed, stringent limitations on the collection, use, retention, and disclosure of information are arguably appropriate. Existing law establishes a precedent for enhanced privacy concerning PI collected in an educational setting, and proctoring services, in order to ensure fidelity in test-taking, are, by definition surveillance technology. In many cases, proctoring services are also generally used to monitor test-taking for students engaged in remote learning from their home, where students maintain a reasonable expectation of privacy. The possibility that extraneous information regarding the goings-on of the student's household is captured seems to necessitate stronger privacy protections than are generally applicable to student PI.

Additionally, proponents argue that students subjected to proctoring services in educational settings are not provided the opportunity to withhold consent for the collection of their PI. As the bill's sponsors explain:

> Students often must use this software to complete their academic studies – there are no other options. Yet there are no guardrails protecting students from overbroad data collection. […] Students rarely can opt out of data collection when using remote proctoring, let alone say they don't want to use an online proctoring platform. Rather, the choice is often between using the invasive software or not taking the exam and getting a zero. One study showed that 97% of students using online proctoring tools were required to do so. […] Technology in our schools should help students and foster safe learning environments. Remote proctoring has done neither.

In support of the bill, Immigrants Rising highlights the particular issues this poses for the undocumented population, adding:

> While this information is invasive for all students, <u>it is especially invasive for undocumented individuals.</u> These kinds of requirements have had a chilling effect on the participation of undocumented people in taking these exams. Without clear assurances and accountability about how long their data will be retained – or with whom it will be shared – students do not feel comfortable sharing biometric data. This lack of clarity limits their academic careers and prevents communities statewide from tapping into their valuable skills and important services.

While the additional protections provided by this bill are arguably justifiable, the bill does present some ambiguity as to scope of its provisions. For instance, the bill fails to define the term "proctoring service," leaving it unclear whether the bill applies only to online or remote proctoring services, or whether it also applies to the collection of information by in-person proctors. Additionally, while a standard of "strictly necessary" in the context of data minimization is not unprecedented, precisely what PI is strictly necessary to provide a proctoring service is not clear-cut. As such, absent further clarification of these terms, the bill's enforcement through a private right of action may yield extensive litigation requiring

courts to adjudicate their definitions. Still, the bill appears to occupy an expanding and under-protected niche of student privacy that warrants protection.

6) **"Consistent with and further[ing] the purpose and intent of" the CPRA**: Of relevance to this bill, because the CPRA resulted from a ballot proposition, it generally constrains the ability of the Legislature to modify its provisions. Unless otherwise specified within the proposition, the California Constitution prohibits legislative amendment of statutes created by ballot propositions unless a subsequent proposition is approved by the voting public to do so. (Cal. Const. art. II Sec. 10(c).) Proposition 24 permits changes to the CPRA by the Legislature if the amendment is passed "by a vote of a majority of the members of each house of the Legislature and signed by the Governor," but only if "such amendments are consistent with and further the purpose and intent of this Act as set forth in Section 3 [of the proposition…]."[2]

   Proposition 24 briefly defines the purpose and intent of the CPRA as follows:

   > In enacting this Act, 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.[3]

   The proposition goes on to include several principles intended to guide the implementation of the CPRA, including with respect to consumer rights, the responsibilities of businesses, and the implementation of the law generally. These principles include the following guidance:

   > Businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared. […] Businesses should be held accountable when they violate consumers' privacy rights, and the penalties should be higher when the violation affects children.

   This bill provides that a proctoring service shall only collect (and retain, use, and disclose) consumers' PI to the extent it is strictly necessary to provide the proctoring service, which seems to clearly further the specified purpose of Proposition 24 to limit collection of consumer PI to the extent that it is relevant and necessary in relation to the purposes for which it is being collected, used, and shared. Additionally, while the private right of action provided by the bill differs from the general enforcement mechanism for most provisions of the CPRA (excluding the data breach provisions), it would seemingly provide for significant accountability on the part of proctoring services should they violate the privacy rights of students. For these reasons, the amendment to the CPRA proposed by SB 1172 does not seem to violate the restrictions placed on amendments to the CPRA by Proposition 24, since it appears in accordance with the purpose and intent of the law, as described, and thus meets the requirements for amendment by an act of the Legislature.

   Nonetheless, for reasons detailed in the following comment, the author has agreed to an amendment to relocate the provisions of this bill out of the CPRA and into the Business & Professions Code, where it is arguably a more logical fit. No courts have yet weighed in on whether the amendment constraints imposed by Proposition 24 apply to legislation outside

---

[2] Ballot Pamp., Primary Elec. (Nov. 3, 2020) Text of Proposed Laws, pp.74-75; Emphasis added.
[3] *Id.*, at pp. 43-44.

the text of the CPRA, but whether or not this is the case, SB 1172 does not appear to be at significant risk of violating those constraints.

7) **The Business & Professions Code, rather than the CPRA, is arguably a more appropriate placement for the provisions of this bill**: By requiring stringent data minimization, this bill would establish strong protections for the privacy of students who are subject to proctoring services in educational settings. However, the narrow circumstances to which this bill applies, both technologically and contextually, seem to contrast with the industry- and technology- agnostic approach of the CCPA/CPRA, which provides general baseline data privacy protections.

A coalition in opposition to the bill consisting of California Chamber of Commerce, Civil Justice Association of California, TechNet, and California Asian Pacific Chamber of Commerce argues:

> [The CCPA] was designed to provide uniform protections for all forms of [PI] in a comprehensive, industry- and technology- neutral manner, and was heavily negotiated to include only a limited private right of action for data breaches of PI. Notably, voters preserved that framework, including the limited PRA, when they approved the CPRA in Proposition 24 (2020). […]
>
> The broader business community shares significant concerns that: (1) there will be longer-term ramifications of inserting new civil actions into the privacy law before it has been fully operationalized; and (2) SB 1172 will be the first of many bills to revert to the pre-2018 approach of enacting one-off statutes to enact new privacy protections for specific industry or technologies. Such a piecemeal approach to privacy protections, where the Legislature picks and chooses new industries or types of PI to adhere to separate rules, will complicate implementation and undermine the purpose and efficacy of the landmark, comprehensive privacy law.

While it is true that the CCPA provides minimum protections for PI generally, it does not appear to be the case that the CCPA was designed to impose uniformity by foreclosing the possibility of additional protections for specific cases of particularly sensitive information. Rather, the CCPA seems to explicitly leave room for further regulation in circumstances in which more extensive protection is necessary. Specifically, the CCPA includes provisions indicating that its protections for consumer privacy and data control should be interpreted broadly and should be in addition to, not in the place of, more specific consumer protections as circumstances demand. Section 1798.194 of the Civil Code, for instance, provides that the CCPA "shall be liberally construed to effectuate its purposes," and Section 1798.175 of the Civil Code further provides:

> [The CCPA] is intended to further the constitutional right to privacy and to supplement existing laws relating to consumers' personal information […] Wherever possible, law relating to consumers' personal information should be construed to harmonize with provisions of [the CCPA], but in the event of a conflict between other laws and provisions of [the CCPA], the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Furthermore, the CPRA explicitly provides for amendment of its general privacy provisions so long as those changes further the protection of consumer privacy. Accordingly, it does not

seem that privacy laws that supplement the protections provided in the CCPA/CPRA in cases of particular sensitivity conflict with the purpose and intent of either the CCPA or the pending CPRA.

That said, while the CCPA and CPRA do not appear to foreclose additional, case-specific privacy protections elsewhere in law in sensitive circumstances, the CCPA and CPRA are designed to be generally applicable. As such, inserting industry- or technology- specific provisions within the text of the CPRA arguably raises several concerns, including complicating interpretation of its general provisions. Inserting such provisions into the text of the CPRA may also encourage future legislation to take a similar approach, compromising the readability of the CPRA by smattering standalone provisions within a law intended to provide a general baseline.

The CPRA is one of many statutes within the Civil Code that addresses a category of information, in this case consumer PI collected by businesses. Other privacy statutes within the Civil Code similarly deal with categories of information, providing protections for medical information, customer records, financial and credit information, driver's license information, and electrical and natural gas usage information, among others. On the other hand, while the Business & Professions Code similarly contains several privacy statutes, these statutes are instead largely targeted toward particularly industries or services, rather than categories of information. For instance, SOPIPA regulates operators of educational technology services designed and marketed for K-12 purposes, and neighboring provisions regulate operators of educational technology services designed and marketed for children enrolled in preschool and prekindergarten, operators of online services targeted to minors, and operators of commercial websites generally.

Based on the similarity between the provisions of this bill and the privacy laws residing in the Business & Professions Code, along with concerns regarding the interpretability and readability of the CPRA, it is therefore arguably more appropriate that the provisions of this bill be placed alongside SOPIPA and other similar privacy protections. Accordingly, the author should amend the bill as follows to relocate its provisions to the Business & Professions Code.

Amendment:

On page 2, line 1, strike "Section 1798.101" and insert "***Chapter 22.2.7***"; strike "Civil" and add "***Business and Professions***".

On page 2, after line 2, insert: "***CHAPTER 22.2.7: Student Test Taker Privacy Protection Act***"

On page 2, line 3, strike "1798.101" and insert "***22588****"*; strike "subdivision (a) of".

On page 2, line 4, strike "1798.100 and paragraph (6) of subdivision (a) of Section 1798.145" and insert "***22584***".

The CCPA and CPRA both contain lengthy sections dedicated to defining critical terms and enumerating exemptions from the law's requirements. (*See* Civ. Code Secs. 1798.140 and 1798.145, respectively.) Consequent to the aforementioned amendment removing the provisions of SB 1172 from the CPRA and placing them in the Business & Professions Code,

the definitions and exemptions from the CPRA would no longer apply to the bill by default. As a result, adopting that amendment arguably necessitates explicit definition of terms and exemptions within the text of SB 1172. Toward this end, the author should adopt the following amendment, which would preserve the applicability of the definition of "personal information" from the CPRA, and would provide similar exemptions to those available in the CPRA to ensure the protections of the bill do not jeopardize health, safety, and other available rights under law.

Amendment:

On page 2, after line 15, insert: "***(c) This section shall not prohibit a business from collecting, using, retaining, or disclosing personal information if doing so is necessary for any of the following:***

(1) To comply with a requirement of federal, state, or local law

(2) To comply with a court order or subpoena.

(3) 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 such an inquiry or investigation, or authorized to serve a subpoena or summons, as applicable. A law enforcement agency may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court order or subpoena to obtain the consumer's personal information. A business that has received direction from a law enforcement agency not to delete a consumer's personal information that otherwise would not be permissible to retain or disclose pursuant to this section shall not use or disclose the consumer's personal information for any purpose except in response to a court order or subpoena.

(3) 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.

(4) 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:

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

(B) 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.

(C) 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.

(5) To exercise or defend a legal claim.

(d) For the purposes of this section, "personal information" has the same meaning as in Section 1798.140 of the Civil Code."

8) **Bill would provide a private right of action for aggrieved consumers to recover damages and seek injunctive or declaratory relief**: This bill would allow a consumer whose PI is collected, used, retained, or disclosed beyond what is strictly necessary to provide the proctoring service to bring a civil action against the business. The bill specifies that a consumer who brings such a civil action may recover all of the following: liquidated damages of $1,000 per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; and reasonable attorney fees and costs, including expert witness fees. In support of the bill, and the private right of action therein, ACLU California Action argues:

> Current law does not offer enough protection to students subject to remote proctoring, so we need stronger protections for Californians. We also need to give students tools to fight back against irresponsible companies. SB 1172 not only gives students the control they deserve over their own biometric and other private information, but it also empowers test takers to protect their privacy rights against proctoring services by providing a private right of action against proctoring companies.

On the other hand, opponents of the bill contend that the private right of action provided by this bill would result in frivolous and predatory lawsuits, and is antithetical to the agreement underlying the passage of the CCPA. In opposition to the bill, Meazure Learning, DBA ProctorU, argues:

> Adding a private right of action to recover liquidated damages of $1,000 per consumer per incident or actual damages is contrary to the fundamental agreement that was reached with the Legislature on the CCPA. Specifically, that in exchange for a regulated privacy regime enforced by the California Attorney General's Office that [*sic.*] there would not be a private right of action. This legislation clearly would allow for an exception even before the regulatory structure has been finalized.
>
> SB 1172 will lead to unintended consequences not only for proctoring services, but also for numerous educational institutions who utilize any type of proctoring service and third parties that support the provision of proctoring services. This fundamental change will likely lead to frivolous lawsuits against educational institutions, online and in-person proctoring service providers, and any other third party that supports them.
>
> Additionally, the bill as written is ambiguous on which personal information is "strictly necessary" to provide those services. This leaves the interpretation of "strictly necessary" to the discretion of the courts and creates an incentive for trial attorneys to argue that *any* personal information processed in collection with proctoring services is not "strictly necessary."

This bill has been double-referred to the Assembly Judiciary Committee, where the bill will be analyzed should it pass out of this Committee. The Assembly Judiciary Committee has historically been responsible for analyzing the appropriateness of private enforcement across a broad range of issues. While the enforcement mechanism provided by this bill is a critical policy consideration, in this case, it is arguably more appropriately addressed by the committee of second referral based on jurisdictional precedent.

9) Related legislation: SB 746 (Skinner, 2022) would amend the CCPA to require, upon request, that businesses to disclose to consumers whether they use the PI of consumers for political purposes, as defined, and would require the same disclosure annually to the Attorney General or the California Privacy Protection Agency.

SB 1454 (Archuleta, 2022) would remove the sunset on the exemption from certain provisions of the CCPA for PI reflecting communications or transactions between businesses and other entities that occur solely within the context of the business conducting due diligence or providing or receiving a product or service; and would remove the sunset on the exemption from certain provisions of the CCPA for PI that is collected and used by a business solely within an employment context.

AB 2871 (Low, 2022) is identical to SB 1454.

AB 2891 (Low, 2022) would extend the sunsets specified in SB 1454 and AB 2871 until January 1, 2026, rather than removing them.

AB 2355 (Salas, 2022) would require a local educational agency (LEA) to report cyberattacks impacting more than 500 pupils or personnel to the California Cybersecurity Integration Center (Cal-CSIC), and would require Cal-CSIC to track and annually report to the Legislature on cyberattacks and data breaches affecting LEAs.

10) Prior legislation: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment #4.

AB 2799 (Chau, Ch. 620, Stats. 2016) *See* Comment #4.

SB 1177 (Steinberg, Ch. 839, Stats. 2014) *See* Comment #4.

REGISTERED SUPPORT / OPPOSITION:

Support

Electronic Frontier Foundation (sponsor)
Privacy Rights Clearinghouse (sponsor)
ACLU California Action
California Medical Association
CalPIRG, California Public Interest Research Group
Center for Digital Democracy
Citizens Privacy Coalition of Santa Clara County
Common Sense
Consumer Action
Consumer Federation of America
Consumer Reports
Electronic Privacy Information Center (EPIC)
Fairplay
Fight for The Future
Greenlining Institute
Immigrants Rising
Media Alliance

Oakland Privacy
Parent Coalition for Student Privacy

Opposition

California Asian Pacific Chamber of Commerce
California Chamber of Commerce
Civil Justice Association of California
Meazure Learning, DBA ProctorU
TechNet

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200