Date of Hearing: March 12, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1971 (Addis) – As Amended March 4, 2024

SUBJECT: Student Online Personal Information Protection Act: administration of standardized tests.

SYNOPSIS

Existing law, the Student Online Personal Information Protection Act (SOPIPA) establishes privacy protections for students in California's K-12 public schools. The California Consumer Privacy Act (CCPA) offers additional privacy protections for consumers of all ages when it comes to the personal data collected by large businesses. Despite these protections, the cumulative protections in SOPIPA and the CCPA have not stopped the sale of students' private information by non-profit organizations that are advertised as helping students prepare for college.

To prevent the sharing and sale of student's personal data, either by the College Board and other non-profit college preparation and standardized testing organizations, or by the post-secondary institutions that those businesses share the students' personal data with, this bill does two important things. Under SOPIPA, this bill:

1. *Prohibits operators from sharing students' information with post-secondary institutions without first obtaining consent from the student, if at least 18 years old, or their parents or guardians, if under 18 years old.*

2. *Expands the current definition of "for K-12 purposes" to include the administration of standardized tests taken to bolster a student's chances of admission, as well as tests taken to prepare for those standardized tests.*

According to an investigative report by Consumer Reports in 2019, the College Board collected and relayed personal student information to companies such as Facebook, Google, Microsoft, Snapchat, Adobe, Yahoo, and others. Among the personal data shared with these companies were usernames and unique identifiers, which can be used to track student activity across websites beyond the College Board website. At the time of the report, the College Board's own privacy policy stated that they did not share any personally identifiable information (the same policy classified usernames as personal information). The investigation also found that much of the personal information shared with 3rd party entities was later used for 'behavioral targeted advertising' to those same students.

The evidence discussed in this analysis strongly supports the need for the changes contained in this bill. Closing this loophole when it comes to protecting the private information of students and their parents furthers California's privacy goals.

This bill is author sponsored and supported by Oakland Privacy. If passed by this Committee, this bill will next be heard by the Assembly Education Committee.

SUMMARY: Prohibits an operator under the Student Online Personal Information Protection Act (SOPIPA) from sharing information with a post-secondary institution without consent. Specifically, **this bill**:

1) Prohibits an operator from knowingly sending information to a postsecondary institution for the purpose of facilitating the pupil's admission to that institution, without first obtaining consent.

2) Expands the definition of "K-12 school purposes" to include the administration of a standardized test for the purpose of either bolstering a student's application for admission to a postsecondary institution, or preparing for that standardized test.

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) Establishes the Student Online Personal Information Protection Act (SOPIPA), which prohibits an operator of a website, online service, online application, or mobile application from knowingly engaging in targeted advertising to students or their parents or legal guardians using covered information, as defined, amassing a profile of a K-12 student, selling a student's information, or disclosing covered information, as provided. (Bus. & Prof. Code §§ 22584-85.)

3) Defines an "operator" to mean the operator of an internet web site, 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. (Bus & Prof. Code § 22584(a).

4) Defines "K-12 school purposes" as those that customarily take place at the direction of the K-12 school, teacher, or district or aid in the administration of school activities. (Bus. & Prof. Code § 22584(b)(4))

5) Defines "covered information" as personally identifiable information or materials, in any media or format that meets any of the following:

   a) It is created or provided by a pupil, or the pupil's parent or legal guardian, to an operator in the course of the pupil's, parents', or legal guardian's use of the operator's site, service, or application for the school's purposes.

   b) It is created or provided by an employee or agent of the preschool, prekindergarten, school district, local educational agency, or county office of education, to an operator.

   c) It is gathered by an operator through the operation of a site, service, or application, as defined in number 7, and is descriptive of a pupil or otherwise identifies a pupil, including, but not limited to, information in the pupil's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic

information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. (Bus. & Prof. Code §§ 22584(i) and 22586(i).)

6) Requires an operator of a commercial website or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its website to conspicuously post its privacy policy. (Bus. & Prof. Code § 22575.)

7) Protects, pursuant to the federal Family Educational Rights and Privacy Act (FERPA), the confidentiality of educational records meaning those records, files, documents, and other materials which, (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution by prohibiting the funding of schools that permit the release of those records. FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. FERPA's prohibition only applies to the school itself and contains various exemptions allowing the data to be released without the written consent of the parents. (20 U.S.C. § 1232g(b)(1).)

8) 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 personal information 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. § 6502.)

9) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

10) Provides that the CCPA applies to any for-profit entity that collects consumers' personal information, does business in California, and meets one or more of the following criteria:

    a) It had gross annual revenue of over $25 million in the previous calendar year.

    b) It buys, receives, or sells the personal information of 100,000 or more California residents, households, or devices annually.

    c) It derives 50% or more of its annual revenue from selling California residents' personal information. (Civ. Code § 1798.140(d).)

11) Prohibits a business from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of those who are between 13 and 16 years of age, or the consumers parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the information. (Civ. Code § 1798.120.)

12) Defines "consumer" as a natural person who is a California resident. (Civ. Code § 1798.140(i).)

13) 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. Personal information includes such information as:

    a) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

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

    c) Biometric information.

    d) Internet activity information, including browsing history and search history.

    e) Geolocation data.

    f) Professional or employment-related information. (Civ. Code § 1798.140(v).)

14) Defines "sensitive personal information" as personal information that reveals:

    a) A consumer's social security, driver's license, state identification card, or passport number.

    b) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

    c) A consumer's precise geolocation.

    d) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

    e) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

    f) A consumer's genetic data. (Civ. Code § 1798.140(ae).)

15) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

    a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

    b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.120.)

e) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

16) Limits a business providing test proctoring services in an educational setting to collecting, using, retaining, and disclosing only the personal information strictly necessary to provide those services. (Bus. & Prof. Code §22588(a).)

FISCAL EFFECT: As currently drafted, this bill is keyed non-fiscal.

COMMENTS:

1) **Purpose of this bill.** Existing law, the Student Online Personal Information Protection Act (SOPIPA) establishes privacy protections for students in the California's K-12 public schools. In addition, the California Consumer Privacy Act (CCPA) offers additional privacy protections for consumers of all ages when it comes to the personal data collected by large businesses. Despite these protections, a significant loophole exists when it comes to information collected by non-profit standardized test administrators, such as the College Board.

Specifically, there is ambiguity related to the entities SOPIPA applies to, with the existing definition being an "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." Specifically, the author argues that the definition of "primarily used for K-12 purposes" has led to some entities, primarily standardized testing organizations, to determine that the protections that SOPIPA gives to California's students does not apply when it comes to the personal information they are collecting.

In addition, as noted in the EXISTING LAW section, the CCPA requires business that meet the following criteria to protect consumers' private information:

1. Had gross annual revenue of over $25 million in the previous calendar year.

2. Buys, receives, or sells the personal information of 100,000 or more California residents, households, or devices annually.

3. Derives 50% or more of annual revenue from selling California residents' personal information.

While it is likely that the College Board would meet the criteria under one and two, the CCPA applies to large for-profit businesses and excludes non-profit organizations, regardless of their size.

The purpose of this bill is to expand the SOPIPA definition of "primarily used for K-12 purposes" to include standardized testing for the purpose of college admissions, in order to ensure that the personal data collected by non-profit standardized test administrators is subject to all of the protections included in the Act, including a prohibition against selling or sharing specific covered information. [See EXISTING LAW section for more information.]

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

> There is a clear and concerning lack of protections for California's students when it comes to their data privacy. Advances in technology, including artificial intelligence, have surpassed our state's privacy laws, leaving our students vulnerable to irresponsible uses of their personal data. As technology continues to progress, so should the protections provided to Californians. AB 1971 will ensure that every student's data is protected throughout their educational careers.

3) **Background.** The College Board is a large, non-profit company that owns and administers the SAT suite of tests, including the Preliminary SAT / National Merit Scholarship Qualifying Test (PSAT/NMSQT). In addition, the Board manages other tests, including Advanced Placement (AP) tests, and offers a number of services to help students and their families make decisions about secondary education.[1] There have multiple instances of the College Board using individualized K-12 student data in ways that would have violated SOPIPA and the CCPA.

According to an investigative report from Consumer Reports in 2019, the College Board was collecting and relaying personal student information to companies like Facebook, Google, Microsoft, Snapchat, Adobe, and Yahoo, among others. Among the personal data shared with these companies was usernames and unique identifiers, which can be used to track student activity over multiple websites, not just the College Board site. At the time, the College Board's own privacy policy stated that they did not share any personally identifiable information (the same policy classified usernames as personal information). The investigation also found that much of the personal information shared with 3rd party entities was then used for 'behavioral targeted advertising' to those same students.[2]

The New York Times, in 2018, conducted an investigation into the College Board and ACT's collection and dispersion of student information provided in online surveys designed to match students with colleges they might be interested in. Their investigation found that both companies charged educational institutions approximately 45 cents per name to allow access to the information provided by over 3 million high school juniors who took the surveys. In the Times article, Joel Reidenberg, a professor at the Fordham University School of Law noted, "The harm is that these children are being profiled, stereotyped, and their data profiles are being traded commercially for all sorts of uses — including attempts to manipulate them and their families."[3]

4) **The California Consumer Privacy Act (CCPA).** In 2018, the Legislature enacted the California Consumer Protection Act (CCPA) (AB 375 (Chau, Chap. 55, Stats. 2018)), which

---

[1] The College Board website can be found here: https://www.collegeboard.org/.
[2] Fitzgerald, Bill. "Student Tracking and the College Board" *Medium* (Jul 30, 2020) *available at* https://medium.com/@funnymonkey/student-tracking-and-the-college-board-512a94d60ec3.
[3] Singer, Natasha. "For Sale: Survey Data on Millions of High School Students." *The New York Times* (Jul 29, 2018) *available at* https://www.nytimes.com/2018/07/29/business/for-sale-survey-data-on-millions-of-high-school-students.html,

gives consumers certain rights regarding their personal information, such as: (1) the right to know what personal information that is collected and sold about them; (2) the right to request the categories and specific pieces of personal information the business collects about them; and (3) the right to opt-out of the sale of their personal information, or opt-in, in the case of minors under 16 years of age. The CCPA was the byproduct of compromises made between business interests on one side, and consumer and privacy interests on the other, to provide a legislative alternative to a ballot initiative on the same subject.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which established additional privacy rights for Californians. With the passage of the CCPA and the CPRA, California now has the most comprehensive laws in the country when it comes to protecting consumers' rights to privacy.

In addition, Proposition 24 created the California Privacy Protection Agency (Privacy Agency) in California, vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA and the CPRA. The Agency's responsibilities include updating existing regulations, and adopting new regulations.

To protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy. (Ballot Pamphlet., Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74.) While this bill does not amend the contents of the CPRA, it is consistent with the intent by insuring that the constitutional right to privacy is enhanced, since data regarding citizenship and immigration status will have heightened protection if this bill is enacted.

Importantly, the CPRA included additional restrictions on information that is considered "sensitive personal information." When it comes to personal information, consumers have the four rights outlined above. However, when it comes to the use of their sensitive personal information, consumers have the right to further restrict a business's use and disclosure of that information. Specifically, a person has the right to restrict a business's use of their sensitive personal information to "that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services." (Civ. Code § 1798.121(a).)

5) **How this bill would work.** To protect the sharing and sale of student's personal data either by the College Board and other college preparation and standardized testing non-profit organizations or the post-secondary institutions that those businesses share the students' personal data with, this bill does two important things:

1. Prohibits operators from sharing students' information with post-secondary institutions without first obtaining consent from the student, if 18 or over, or their parents or guardians, if under 18.

2. Expands the current definition of "for K-12 purposes" to clarify that it includes the administration of both standardized tests that are taken to bolster a student's chances of admission, and tests taken to prepare for those standardized tests.

6) **Analysis.** In general, state law in the form of SOPIPA protects the personal information collected about students in the state's public schools. However, as discussed previously, there is ambiguity related to the entities SOPIPA applies to, which leaves room for non-profit college preparatory businesses to share and sell the personal information of the millions of students who take their tests, respond to their surveys and provide detailed information in order to identify potential colleges and universities. Along with SOPIPA, California has some of the most robust privacy protection laws in the nation under the CCPA. Unfortunately, the cumulative protections in SOPIPA and the CCPA were not sufficient to stop the sale of students' private information by non-profit organizations that are advertised as helping students prepare for college.

The author makes a compelling point when she notes:

> The College Board is uniquely situated in the realm of K-12 education and should be subject to the same data restrictions as other K-12 entities. The College Board essentially act as gatekeepers to higher education, providing services and tests that give students a massive advantage in college admissions over those who choose not to participate. Over 500,000 California students took the SAT in 2023, with 122,000 of those being seniors. While some institutions of higher education have removed the requirement for prospective students to submit their SAT scores, there has been a recent movement from many private institutions to reinstate that requirement.
>
> The College Board also oversees the administration of AP testing, which over 1.8 million students participated in nationwide. The vast majority of students who take AP courses use the College Board website to access their test scores and other resources, giving the College Board (and potentially 3rd party entities) access to sensitive student data with almost no safeguards.

In addition, *Oakland Privacy*, provides this additional evidence in their letter in support of the bill:

> Earlier this month, the New York Attorney General's Office under AG Leticia James, assessed the nonprofit College Board a $750,000 fine. The NYAG found that the nonprofit was soliciting student data not required to administer examinations, including student GPA, area of anticipated study, interest in a religiously affiliated college and family income, and selling that information to over 1,000 clients, primarily institutes of higher education. Moreover, the NYAG investigation also found that the College Board used test sign-up processes to solicit student data for its own marketing services and to gather more information to sell.

The evidence provided strongly supports the need for the changes contained in this bill. Closing this loophole by protecting the private information of students and their parents furthers California's privacy goals.

Finally, it is important to note that the information provided in these surveys, especially those targeted at finding possible scholarships, can contain very sensitive personal information, including information related to the student or their family's immigration status. Therefore this bill is consistent with California's public policy goals of respecting and protecting Californians who are immigrants. California's recent history has been one of inclusion and respect for our immigrant neighbors. While Congress has failed to pass comprehensive immigration reform, California has exercised its state power to protect immigrants who are caught in limbo due to

Washington's inaction. Year after year, the Legislature continues to act by passing significant legislation to both protect people from harm who have immigrated to California, and to provide them with many of the supports and services provided to all California residents. This bill, in keeping with that tradition, endeavors to protect Californians' personal data that might disclose their citizenship and immigration status.

For future consideration. While beyond the scope of this bill, the Committee may wish to consider whether or not the concerns raised about the College Boards' activities warrant modifying the CCPA to include large non-profits. According to *ProPublica*'s Nonprofit Explorer, the College Board reported over $1 billion in revenue in 2022 and approximately $895 million in expenditures. The Explorer also reports that according to their December 2022 tax filings, the company provided first-class or chartered travel to key employees or officers. Finally, according to their records, the College Board had over $2 billion in assets in 2022.[4] This level of revenue and the numbers of consumers they interact with and collect data from on an annual basis far exceeds the thresholds in the CCPA. If all non-profits meeting the existing criteria were required to provide all of the protections that their similarly-sized for-profit siblings a currently providing, if would significantly further the state's goal of protecting Californian's personal data.

7) **Related legislation.** Currently, AB 801 (Joe Patterson) requires an operator of an internet website, online service, online application, or mobile application used primarily for school purposes to delete any personally identifiable information or materials related to a pupil, that is not otherwise covered under the California Consumer Privacy Act (CCPA), at the request of a pupil, parent, or guardian if the child is no longer attending the school or district. That bill is currently in the Senate Rules Committee pending referral.

AB 375 (Chau, Chap. 55, Stats. 2018) established the California Consumer Privacy Act of 2018 which provides consumers the right to access their personal information that is collected by a business, the right to delete it, the right to know what personal information is collected, the right to know whether and what personal information is being sold or disclosed, the right to stop a business from selling their information, and the right to equal service and price.

AB 2799 (Chau, Chap. 620, Stats. 2016) establishes the Early Learning Personal Information Protection Act which prohibits operators of Internet Web sites, online services, and mobile apps that are designed, marketed and used primarily for prekindergarten and preschool pupils, from using data about those pupils for targeting, marketing or profiling, and prohibits selling or disclosing a pupil's information with limited exceptions.

SB 1172 (Pan, Chap. 770, Stats. 2022) prohibits a business providing test proctoring services in an educational setting from collecting, retaining, using, or disclosing personal information except to the extent necessary to provide those proctoring services and in other specified circumstances.

SB 1177 (Steinberg, Chap. 839, Stats. 2014) established the Student Online Personal Information Protection Act to restrict the use and disclosure of information about K-12 students.

REGISTERED SUPPORT / OPPOSITION:

Support

---

[4] Information on the *ProPublica* Nonprofit Explorer can be found *here*: https://projects.propublica.org/nonprofits/.

Oakland Privacy

Opposition

None on this committee's file.

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200