Date of Hearing: July 16, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 435 (Wahab) – As Amended June 23, 2025

SENATE VOTE: N/A

PROPOSED AMENDMENTS

SUBJECT: California Consumer Privacy Act of 2018: sensitive personal information

SYNOPSIS

The Legislature enacted the California Consumer Privacy Act (CCPA) in 2018 and the voters amended it by an initiative measure, the California Privacy Rights Act (CPRA), in 2020. The CPRA introduced the concept of "sensitive information" – such as social security numbers, credit card numbers, geolocation, sexual orientation, immigration status, and certain health information – and granted consumers the right to restrict the use of such information on a business-by-business basis and, like personal information, provided that consumers may "opt out" of the sharing and sale of such information. Since the passage of the CPRA, 17 states have passed privacy laws with stronger protections, including one that prohibits sharing of sensitive information entirely and 16 that require consumers to "opt in" to the sharing and sale of personal information – thereby making the privacy of the most intimate personal information the default in those states.

A broad exception to the definitions of "personal information" and "sensitive information," expanded by the CPRA, appears to weaken California's privacy protections. That exception is for "publicly available information," defined as information that (1) is made lawfully available from government records, (2) a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or (3) is made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

Arguing that this exception gives businesses nearly unfettered license to monetize sensitive information of vulnerable communities, including immigrants, LGBTQ+ individuals, and children, the author recently amended this bill in its entirety to eliminate the publicly-available exception to "sensitive information," in order to ensure that the limited protections accompanying this status, should a consumer opt to exercise them, are more consistently observed by businesses.

This bill is supported by the Alliance for Children's Rights, Asian Americans Advancing Justice Southern California, and Courage California. It is opposed by the Chamber of Commerce, TechNet, TechCA, and the Computer and Communications Industry Association. The Committee has recommended one technical amendment discussed in Comment #7.

THIS BILL:

1) Deletes the exemption for public information from the definition of "sensitive personal information."

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." (U.S. Const., Fourth Amend; *see also* Cal. Const. art. 1, § 13.)

2) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

3) States that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them." Further states these findings of the Legislature:

    a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

    b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

    c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798.1.)

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

5) Prohibits a business from selling or sharing the personal information of a child that is 16 years of age or younger, if the business has actual knowledge of the child's age, unless the child, or the child's parent or guardian in the case of children less than 13 years old has affirmatively authorized the sharing of selling of the personal information. (Civ. Code § 1798.120(c).)

6) 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. (Civ. Code § 1798.12.)

e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

f) 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.)

7) 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 consumers at least 13years of age and less than 16 years of age, or the consumer's 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 consumer's personal information. (Civ. Code § 1798.120 (c).)

8) States that both personal information and sensitive personal information that is "publicly available" is not considered personal or sensitive. (Civ. Code § 1798.140,)

9) Defines the following terms under the CCPA:

a) "Personal information" means 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:

i) 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.

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

iii) Biometric information.

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

v) Geolocation data.

vi) Audio, electronic, visual, thermal, olfactory, or similar information.

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

b) "Publicly available" means any of the following:

i) Information that is lawfully made available from federal, state, or local government records.

ii) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

iii) Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. (Civ. Code § 1798.140(v)(2)(B).)

c) "Sensitive personal information" means:

i) Personal information that reveals:

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

(2) 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.

(3) A consumer's precise geolocation.

(4) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

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

(6) A consumer's genetic data.

(7) A consumer's neural data.

(a) "Neural data" means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.

(8) The processing of biometric information for the purpose of uniquely identifying a consumer.

(9) Personal information collected and analyzed concerning a consumer's health.

(10) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

10) States that "personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v)(2)(A).)

11) States that "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. (Civ. Code § 1798.140(v)(2)(B).)

12) Requires a business to provide clear and conspicuous links on its homepage allowing consumers to opt-out of the sale or sharing of their personal information and use or disclosure of their sensitive personal information. (Civ. Code § 1798.135(a).)

13) Establishes the California Privacy Protection Agency (Privacy Agency), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

14) Establishes the Data Broker Registration Law (DBRL). (Civ. Code §§ 1798.99.80-1798.99.88.)

15) Defines a "data broker" as a business that knowingly collects and sells the personal information of a consumer to a third party that the business does not have a direct relationship with. (Civ. Code § 1798.99.80.)

16) Requires data brokers to register annually with the California Privacy Protection Agency (CPPA) and provide specified information. (Civ. Code § 1798.99.82.)

17) Requires the CPPA, by January 1, 2026, to develop an accessible deletion mechanism that allows a consumer to request that every registered data broker delete any personal information held by the broker. (Civ. Code § 1798.99.86.)

COMMENTS:

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

> As California becomes more dependent on technology, the companies we share our sensitive personal information with have an obligation to ensure it is safeguarded at all times.
>
> Currently, the California Consumer Privacy Act (CPPA) allows data brokers and corporations to sell & share sensitive personal information they consider publicly available. Federal legislation such as the Children's Online Privacy Protection Act fails to prohibit data brokers from selling data belonging to children. As a result, data brokers can legally sell sensitive personal information to government agencies, bypassing legal processes and procedures to request this information. This is especially alarming as governmental agencies are increasingly surveilling and targeting Californians, especially undocumented immigrants and children.
>
> Senate Bill 435 addresses the loophole in the CCPA by changing the definition of "sensitive personal information" that allows it to be considered "publicly available". This single change increases the privacy and security of consumers and prevents data brokers and corporations from selling or sharing sensitive personal information.

2) **Historical perspective.** To fully understand how completely people in California and throughout the country have ceded the right to live their lives in private, free from both government and private surveillance, privacy experts reflect on the concerns raised by federal and state lawmakers 50 years ago when debating the creation of the FBI's National Crime

Information Center's computerized data collection system (NCIC). This database that was so controversial at the time allowed local, state, and federal law enforcement agencies to share personal data related to suspected criminal activities. Congress held "days and days" of hearings over two years. Members warned of the "threat of the dictatorship of dossiers."[1]

During the debates, Senator Barry Goldwater of Arizona lamented, "Where will it end? . . . Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?"[2] Senator Charles H. Percy of Illinois in foreshadowing of what would come to pass in the 21st century warned:

> I hope that we never see the day when a bureaucrat in Washington or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear that is the trend. . . . Federal agencies have become omnivorous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files . . . of unprotected information on millions of Americans.[3]

During the same period when Congress was expressing concern about the erosion of individuals' privacy protections, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution in 1972.[4] Proponents noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[5]

As Oakland Privacy has so eloquently detailed in their support letter for another privacy bill:

> In 1972, in the wake of revelations about the abuses of J. Edgar Hoover's FBI and the Cointelpro program, Californians, by a 62.9% yes vote, added the right to privacy to California's state constitution via Prop 11. ACA 51, introduced by assembly member Ken Cory added privacy to the list of the inalienable rights of the people of the state and replaced the word "men" with the word "people" in the state constitution.
>
> Cory explained:
>
> > *In the face of a cybernetics revolution and the increasingly pervasive amount of information being compiled, it would be highly desirable that our constitution state in clear terms that each person has a fundamental right to privacy… The constitutional amendment would create a positive, inalienable right to privacy and "put the State and private firms on notice that the people have this fundamental right and it can only be abridged when the public concern is an overriding concern.*

---

[1] Citron, Danielle Keats, *A More Perfect Privacy*, 104 Boston University Law Review, 1073–1086 (2024).
[2] *Ibid.*
[3] *Ibid.*
[4] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[5] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.

Cory battled opposition from private industry, the Department of Motor Vehicles and law enforcement, but was eventually able to corral support from 2/3 of both houses of the Legislature. Prop 11 went on the November 1972 ballot with an argument in support from State Senate Majority Leader George Moscone:

> *"The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian."*
>
> *"The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives"* [Citations omitted.]

Arguably, the present is even more of a dictatorship of dossiers than the 92nd and 93rd Congresses and the voters of California envisioned, with not only governments, our own and others, being able to monitor individual's private lives, but virtually every private business or individual with enough resources and technological savvy having access to those dossiers as well. University of Virginia Law Professor, Danielle Citron, warned in an interview with The Guardian in 2022, "We don't viscerally appreciate the ways in which companies and governments surveil our lives by amassing intimate information about our bodies, our health, our closest relationships, our sexual activities and our innermost thoughts. Companies are selling this information to data brokers, who are compiling dossiers with about 3,000 data points on each of us."[6]

Professor Citron continues to raise alarms about the on-going decimation of the right to privacy:

> In the United States, the quantity of personal data collected, used, shared, sold, and stored has grown to the point of international embarrassment. NCIC is one node in the criminal justice and intelligence "information sharing environment." Private- and public-sector databases reveal the most intimate details of people's lives, including their thoughts, searches, browsing habits, bodies, health, sexual orientation, gender, sexual activities, and close relationships. The quantity and quality of personal data being amassed has exceeded all warning; the distinction between public and private collection efforts has vanished; the

---

[6] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) *available at* https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.

> privacy that people want, expect, and deserve has been, and continues to be, under assault.[7] [Citations omitted.]

Catherine Powell, adjunct senior fellow for women and foreign policy at the Council on Foreign Relations, pointed out in 2023 in a blog post for the Council:

> If you've engaged with any form of technology recently—whether through a smartphone, social media, a fitness tracker, even a seemingly innocuous game like Candy Crush—you have accumulated a substantial amount of intimate privacy data. Intimate data ranges from your location, to when you fall asleep, to even more closely guarded information like your menstrual cycle or sexual partners. And every day, this data is scraped, bought, and sold by data brokers to third parties. Beyond violating our privacy, this repurposing of our personal data undermines our security.[8]

3) **California Consumer Privacy Act**. In 2018, the Legislature enacted the CCPA (AB 375; Chau, Chap. 55, Stats. 2018), which gave consumers certain rights regarding their personal information,[9] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt-out of the sale of their personal information, or opt in, in the case of minors under 16 years of age. In addition, the CCPA defined "publicly available" as "information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. This definition excluded biometric information collected by a business about a consumer without the consumer's knowledge. Additionally, under the CCPA passed in 2018, information was not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which both established additional privacy rights for Californians and arguably weakened other privacy rights. Chief among these additional rights was the right of a consumer to limit a business's use of sensitive personal information.[10] However, the CPRA also expanded the exemption for "publicly available" information to include, in addition to lawfully available information from government records, the following:

1. Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

2. Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

The CPRA also removed the provision stating that "publicly available" no longer applies to data that is being used for a purpose that is not compatible with the purpose for which the data is maintained and made available.

---

[7] Citron, 2024.
[8] Powell, Catherine. "Data is the New Gold, But May Threaten Democracy and Dignity," *Council on Foreign Relations* (Jan. 5, 2023) https://www.cfr.org/blog/data-new-gold-may-threaten-democracy-and-dignity-0.
[9] Civ. Code § 1798.140(v). See **EXISTING LAW** #9(a) for definition.
[10] Civ. Code § 1798.140(ae). See **EXISTING LAW** #9(b) for definition.

In addition, the exemption for publicly available personal information was also applied to a new category – sensitive personal information. While these changes to the publicly-available exemption, theoretically, were designed to exempt information that a person posts on a social media platform, proponents of the bill argue that a company could claim that it believed someone's sensitive information was made available to the general public or that the person disclosed the information to a second party and had not requested that the sharing be restricted.

One of the most important components of Proposition 24 was establishing that the CCPA, as amended, was a floor and not a ceiling for privacy protection. Essentially, 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 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.[11]

5) **Challenges with California's privacy laws.** The proponents of the 1972 ballot measure noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[12]

Fifty years later, with the voters' passage of the CPRA, California had the most comprehensive laws in the country when it came to protecting consumers' rights to privacy. Since the passage of the CPRA, however, 19 additional states have passed comprehensive privacy laws. Of those states, 17 have laws that are more privacy protective. 16 states require consumers to "opt in" to the sharing and sale of sensitive information and one state, Maryland, prohibits the sharing of sensitive information entirely.[13] In the states that have come after California, privacy is the default while in California, the ability of businesses to share and profit from the selling of personal information, including sensitive information, is the default.

The CCPA relies on consumers actively exercising their rights to "opt out" of the sharing and sale of their personal information and the sharing, sale and use of their sensitive personal information. The challenge is that in order to exercise those rights, consumers must first find the businesses that have collected their personal information and then find a way to contact the company to exercise those rights. It is likely that the average consumer does not even realize that their personal information is being harvested, used to micro target them for advertising, and sold as a commodity to other companies.

Overall, one could also argue that the State's current privacy laws, including laws protecting Californians from government surveillance and protections against unreasonable searches and seizures without an appropriate court order, fall short of the protections envisioned by the Legislature and the voters in 1972. The proponents argued for a much more stringent level of protection – the right to be left alone. The authors of that proposition promised that adding a

---

[11] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74
[12] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.
[13] A comparison chart of state privacy laws can be accessed at https://45555314.fs1.hubspotusercontent-na1.net/hubfs/45555314/Slides%20and%20one-pagers/US%20state%20law%20comparison%20chart_2024_July_1.pdf.

right to privacy would ensure the protection of "our homes, our families, thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose."[14] In 2025, a person would be hard-pressed to find that level of privacy in their homes, much less in public spaces the moment they step outside.

6) **Analysis.** As it pertains to this bill, elected officials in debating privacy in both the state and federal governments 50 years ago clearly foresaw the future facing the country if people's privacy was not aggressively protected. Unfortunately, one could argue it is unlikely that the voters in 2020 contemplated or understood that people's most sensitive personal information could be shared to hundreds of companies within seconds and could change hands and be coupled with other personal information by thousands of companies in order to create detailed profiles that include every aspect of a person's life.[15]

In addition, it is unlikely that many voters who voted in favor of the CPRA understood that the initiative changed the definition of "publicly available" in a way that potentially created a loophole where companies could argue that the consumer did not expressly restrict the information to only being shared with a specific audience. As a result of that failure, they made the sensitive information publicly available and therefore cannot prohibit a business from using, sharing, or selling data. Fortunately, as noted above, the proponents of the CPRA and the voters understood that the Legislature may need to strengthen the CPRA in order to continue to protect Californians' right to privacy.

The intent of this bill is to more consistently protect sensitive information by, at a minimum, ensuring that even if sensitive personal information appears to be publicly available, it still remains sensitive information and is subject to the provisions in the CCPA that allow consumers to opt out of the use of that information. That approach would arguably be an important step toward improving people's privacy.

The opponents, however, argue that eliminating the publicly-available exemption potentially violates the First Amendment. It should be noted at the outset that it appears the issue was not significant enough to warrant a referral to the Judiciary Committee, which has jurisdiction over bills with clear First Amendment implications. Furthermore, the restrictions at stake are rather modest: status as "sensitive information" under the CCPA enables consumers, on a business-by-business basis, to opt out of the sharing of such information and/or to restrict the scope of its use. And, as a general matter, First Amendment protections in the commercial context are less stringent.[16]

Opposition cites to provisions assuring the public's right to access information from the government.[17] This bill does not appear to implicate that right, which does not speak to a business's right to monetize information obtained from government records. Opposition also

---

[14] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props..
[15] For more information on how information is sold and shared, see Don Marti, et al. "Who Shares Your Information with Facebook? Sampling the Surveillance Economy 2023," *Consumer Reports* (Jan. 2024) https://advocacy.consumerreports.org/research/report-who-shares-your-information-with-facebook/
[16] See *Central Hudson v. Public Svn. Comm'n* (1980) 447 U.S. 557, 562
[17] Cal. Const. Art. 1, § 3 states: "The people have the right of access to information concerning the conduct of the people's business, and therefore, the meetings of public bodies, and the writings of public officials and agencies shall be open to public scrutiny."

cites to cases affirming "the right to receive information and ideas"[18] and "the creation and dissemination of information is speech for First Amendment purposes."[19] It is not clear why these general statements show a specific violation arising from a bill enabling a consumer to request that a business not sell sensitive information, such as their immigration status or sexual orientation, even if the information has, technically, been made publicly available under the broad wording of the exemption. Indeed, biometric information already is not subject to the publicly-available exemption, and there does not appear to be a case holding this exclusion violates the First Amendment. Finally, the opposition argues:

> Lastly, we also note that SB 435 also threatens to decrease privacy protections for consumers by forcing businesses to go through any publicly available information they possess and figure out whether it may contain arguably sensitive personal information. This means having to identify or otherwise link publicly available information to specific consumers, which runs contrary to the CCPA and privacy principles. To make this determination, businesses would have to figure out whom each data point belongs to and then assess whether the data point reveals something sensitive about them. In other words, a business would be put in the position of identifying or linking the data points to particular individuals, at the same that that Section 1798.145(j)(1) expressly states that nothing in the CCPA shall be construed to require businesses to "reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information. At best this causes confusion; at worst it creates a conflict.

Nothing in this bill, however, changes the provisions in the CCPA that exempt businesses from their obligations under the act if they are collecting, using, retaining, selling, sharing, or disclosing consumers' personal information that is deidentified or aggregate consumer information.[20] Further, nothing in this bill changes the fact that consumers are still required to opt out of the use of their sensitive information. So assuming a business gets a request from a consumer asking to opt out of the use, sale, and sharing of their sensitive information, the information would not count as such if it has already been deidentified or aggregated. Given those protections, it is unclear how requiring that publicly available sensitive information still be treated as sensitive information would require the reidentification of deidentified consumer information.

Given these considerations, one could reasonably argue that this bill, which protects a person's most sensitive personal information, whether or not it is publicly available, is consistent with and furthers the purpose and intent of the CPRA, which is to protect California consumers' constitutional right to privacy. A question for this Committee is whether acts such as posting a picture of a visit to one's the country birth or a comment about their relationship means that information is no longer sensitive or theirs to control, but rather is fair game to be scraped and monetized.

7) **Amendments.** The author has agreed to the following clarifying amendment:

> Civ. Code § 1798. 140(v)(2)(B)(ii) "Publicly available" does not ~~**mean**~~ ***include either of the following:***

---

[18] *Stanley v. Georgia* (1969) 394 U.S. 557
[19] *Sorrell v. IMS Health Inc.* (2011) 564 U.S. 552, 570.
[20] Civil Code § 1798.145 (a)(1)(F).

(I) Sensitive personal information.

***(II) B*iometric** information collected by a business about a consumer without the consumer's knowledge.

ARGUMENTS IN SUPPORT: Courage California, writes in support:

> Under current law, the CCPA states sensitive personal information that is "publicly available" is not considered sensitive personal information or personal information. Consequentially, data brokers and corporations can legally sell or share sensitive personal information—including information on children.
>
> Additionally, this loophole allows governmental agencies to bypass the 4th amendment and increasingly surveil Californians, especially undocumented immigrants.
>
> SB 435 will address the loophole in the definition of "sensitive personal information" by removing language that allows this data to be treated as anything less than sensitive & private.

Also arguing in support of the bill, Asian Americans Advancing Justice Southern California writes:

> This bill is essential to protect the digital privacy and physical safety of California's AAPI immigrant communities, especially those who are undocumented or are survivors of abuse and exploitation. With over one in seven Asian immigrants in California estimated to be undocumented, privacy is a matter of livelihood and safety. Under the current framework, gaps in how sensitive information is defined put individuals at risk of having sensitive information such as their immigration status, ethnicity, genetic data shared without meaningful safeguards. Such exposure can lead to devastating outcomes like detention, family separation, or exploitation by malicious actors.
>
> This bill also holds significance for AAPI survivors of domestic violence, human trafficking, and sexual assault. Cultural stigma, language barriers, and immigration-related fears often prevent survivors from seeking help. Weak privacy protections further isolate them by increasing the risk that personal data could be accessed by abusers or inadvertently shared with immigration enforcement. Updating the CCPA to reflect these risks provides a more inclusive, trauma-informed privacy framework that respects the dignity and safety needs of some of California's most marginalized populations.

REGISTERED SUPPORT / OPPOSITION:

Support

Alliance for Children's Rights
Asian Americans Advancing Justice Southern California
Courage California
Oakland Privacy
Secure Justice
Seiu California
Unidosus

Oppose

Association of National Advertisers
California Chamber of Commerce
Computer and Communications Industry Association
Consumer Data Industry Association
Cspra
Insights Association
Software Information Industry Association
State Privacy and Security Coalition, INC.
Techca
Technet

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