Date of Hearing: June 23, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 435 (Wahab) – As Amended June 9, 2026

SENATE VOTE: 39-0

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

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.

The CPRA also broadened a key exception to the definitions of "personal information" and "sensitive information." 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 the latter two categories give businesses nearly unfettered license to monetize sensitive information of vulnerable communities, including immigrants, LGBTQ+ individuals, and children, the author recently amended this bill to modify the definition of "publicly available information" to better ensure that CCPA's protections, should a consumer opt to exercise them, are more consistently observed by businesses. Specifically, the bill would remove the phrase "a business has a reasonable basis to believe" from (2) and altogether delete (3). This brings the provision more closely in line with the initial version of the CCPA, as amended by AB 874 (Irwin, Stats. 2019, Ch. 874).

The previous version of this bill was heard by this Committee in 2025 and failed passage on a 7-5 vote. The bill was granted reconsideration. The bill was recently amended in its entirety to pose a new question related to the CCPA and Californians' privacy rights. As a result, it is being heard in the Committee as though it is a new bill.

This bill is supported by Consumer Reports, Privacy Rights Clearinghouse, Oakland Privacy, and a number of additional civil society organizations. The bill is opposed by a coalition of business organizations including the California Chamber of Commerce, the Consumer Data Industry Association, and TechNet.

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) 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.)

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

7) 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).)

8) 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).)

9) 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).)

10) 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.)

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

12) 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.)

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

14) Requires the Privacy Agency, 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.)

THIS BILL: Narrows the "publicly available" exclusion from "personal information" under the CCPA by:

1) Removing the phrase "a business has a reasonable basis to believe" from the subcategory of "publicly available" information that has been lawfully made available to the general public by the consumer or from widely distributed media.

2) Deleting the subcategory of 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.

COMMENTS:

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

> As Californian's becomes more dependent on technology, providing consumers with the ability to decide what information they want to make publicly available is essential to preserve the privacy, safety, and autonomy to control their personal information.
>
> Currently, the California Consumer Privacy Act (CPPA) allows data brokers and corporations to determine what personal information they consider publicly available. As a result, data brokers can collect in mass any personal information and sell it to the highest bidder, including government agencies which bypass legal processes and procedures to access this information. This is especially alarming as governmental agencies are increasingly surveilling and targeting Californians, especially undocumented immigrants and activist.
>
> Senate Bill 435 addresses the loopholes in the CCPA by amending the definition of "publicly available information," which will enhance consumer privacy and security while establishing clearer boundaries regarding what, when, and how information is considered publicly available.

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]

---

[1] Citron, Danielle Keats, *A More Perfect Privacy,* 104 Boston University Law Review, 1073–1086 (2024).

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]

Presently, California voters face an even greater "dictatorship of dossiers"[6] than their predecessors, with not only global governments' ability to monitor individuals' private lives, but also the near ubiquitous access to these dossiers afforded to private businesses and individuals willing to pay for them. There are more than 4,000 data brokers with dossiers on 98% of the people in the United States.[7] The largest data broker, Acxiom, has more than 10,000 data attributes on over 2.5 billion people in more than 60 countries.[8] The amount of data being collected on people has increased dramatically over the last decade as businesses have figured out how to monetize this natural resource.[9]

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,[10] 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.

---

[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.
[6] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[7] Solove, Daniel J. *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[8] *Ibid.*
[9] *Ibid.*
[10] Civ. Code § 1798.140(v). See **EXISTING LAW** #7(a) for definition.

In addition, the CCPA defined "publicly available" as "information that is lawfully made available from federal, state, or local government records. This definition excluded biometric information collected by a business about a consumer without the consumer's knowledge. With regard to the issue of "publicly available" information, the CCPA, as originally enacted, provided:

> (2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is 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. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

In 2019, AB 874 (Irwin, Stats. 2019, Ch. 874) amended that language as follows:

> "Personal information" does not include publicly available information. For ~~**these purposes,**~~ ***purposes of this paragraph,*** "publicly available" means information that is lawfully made available from federal, state, or local government ~~**records, if any conditions associated with such information.**~~ ***records.*** "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. ~~**Information is 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. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.**~~

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.[11] 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.

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 SB 435 argue that a company could claim that it believed someone's sensitive information was made available to the general public or that the person

---

[11] Civ. Code § 1798.140(ae). See **EXISTING LAW** #7(b) for definition.

disclosed the information to a second party and had not requested that the sharing be restricted. Oakland Privacy explains the challenges in this manner:

> [T]he removal of a bullet point about information made available by the consumer if the consumer has not restricted the distribution of the information [is responsive to] current realities, where information is widely scraped from digital platforms and it is, at best, unclear what if anything, a consumer can do to prevent that scraping. The clause was written as if privacy control mechanisms were crystal clear and fully transparent to consumers who can clearly indicate exactly what they intend. But our reality, especially online and in the wooly world of social media, is nowhere near that cut and dried. A privacy law intended to be protective of our personal information can not be effective if it places a formidable gauntlet in front of a user/consumer that they must cross in order to receive the protections of the law. And we know that users/consumers that are the most vulnerable are often the ones that are poorly positioned to navigate confusing privacy controls and distribution limits successfully, including young people, the elderly and limited English fluency populations.

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.[12]

4) **Publicly available information and privacy in public spaces.** A major problem with US privacy laws, including California's, is its continued embrace of the belief "that anything exposed to the public, or data available to the public, or even information shared with others lacks any privacy interest because it is not totally secret. This flawed understanding of privacy creates two common and severe limitations of privacy law—a failure to protect privacy in public or publicly-available data."[13]

As Professor Daniel Solove notes, "most people do not live like hermits; they engage in their life's activities in places where other people congregate. People expect that their activities are private because they are obscure – others won't be paying attention or watching or listening."[14] As demonstrated throughout this paper, modern surveillance technologies have eroded this sense of obscurity. Contributing to the erosion of any semblance of privacy in public spaces is the notion that information that is "publicly available" is no longer private and becomes fair game.[15]

As Professor Solove warns:

> Companies are scraping vast quantities of personal data from the internet. . . . Scrapers argue that public information is fair game, and many privacy laws permit scraping by excluding publicly available data from their protections. The principle of obscurity, however, emphasizes that just because data is publicly accessible does not mean privacy is forfeited. Although the information may not be secret, its obscurity imposes significant limits on

---

[12] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74
[13] Solove, Daniel J. *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[14] *Ibid.*
[15] Civ. Code § 1798.140(v)(2)(B).

> accessibility. Collecting personal data and making it easily discoverable fundamentally alters the level of privacy associated with that information.[16]

He urges policy makers:

> Rethinking the notion of publicly available information would close a gaping hole in privacy protection; it would prevent companies and the government from vacuuming up vast quantities of personal data; it would protect personal data online with important privacy safeguards and limitations.[17]

5) **What this bill would do.** This bill makes the following changes to the CCPA's definition of "publicly available" information that is excluded from the definition of "personal information":

> Civ. Code Section 1798.140. (v)(2)(B) (i) For purposes of this paragraph, "publicly available" means ~~**any**~~ ***either*** 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.**~~

By narrowing this exclusion from the definition of "personal information," the bill expands the protections of the CCPA to encompass a broader range of information, enabling consumers to more effectively exercise their opt-out and deletion rights. This change is more in line with the "publicly available" definition in the original CCPA. As amended by AB 874 (Irwin, Stats. 2019, Ch. 874), definition applied only to "information that is lawfully made available from federal, state, or local government records."

6) **The need for this bill.** In their support letter, Consumer Reports articulates the challenges with the current definition of "publicly available" information in the CCPA and the need for changes:

> Under the current law, CCPA privacy rights do not apply to "publicly available information" which is defined as:
>
> - information that is lawfully made available from federal, state, or local government records,
> - 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, OR
> - 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.

---

[16] Solove (2025)
[17] *Ibid.*

> The third provision above is the most problematic: under the CCPA, any information you provide to any single other person or company is arguably "publicly available information" — and thus outside the scope of CCPA — unless you specifically instruct the recipient not to provide that information to others. Given the modern data ecosystem where consumers interact with dozens (if not hundreds) of companies every day and there is often no automated or standardized way to restrict resharing, this exception could potentially swallow the whole of CCPA and render it moot. Such an interpretation is clearly inconsistent with the purpose and structure of CCPA which provides opt-out rights over certain processing and sharing of data, but nevertheless grants other rights (such as access, deletion, and correction) over data not subject to such opt outs. SB 435 would fix this inconsistency in the law by eliminating this potential loophole.
>
> The second provision above could also potentially be abused, by imposing a subjective test from the perspective of a company as to whether data has been made publicly available by a consumer or the media. Whether data has been made available or not is an objective matter of fact — it is not the personal opinion of a data broker or advertising company. If a company makes a good faith error as to whether certain data is public or not, it is still an error and should be a technical violation of the law — just as other data processing errors are under the CCPA.

7) **Analysis.** Some may consider sharing their private information, including websites they visit, purchases, employment history, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, failing to actively protect our private information can have real world consequences. As an example, dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal information with advertisers, including location, sexual orientation and mental health details.[18] This was not the first time Grindr had failed to protect their users' private information. Several years earlier, it was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[19]

Catherine Powell in a 2023 blog post for the *Council on Foreign Affairs* highlights the ubiquitous plundering of people's personal, intimate data:

> 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

---

[18] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[19] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.

> data brokers to third parties. Beyond violating our privacy, this repurposing of our personal data undermines our security.[20]

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. Since that time, Californians' privacy rights have been slowly chipped away until they have largely disappeared. One could argue it is unlikely that the voters in 2020 when voting on the CPRA 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.[21]

Given these considerations, one could reasonably argue that this bill returns the meaning of publicly available to one that is commonly understood 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 country of 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.

Opposition cites to provisions assuring the public's right to access information from the government: "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."[22] But nothing about this right guarantees the ability to monetize personal information.

Additionally, opposition cites *Sorrell v. IMS Health Inc*,[23] for the proposition that "the creation and dissemination of information is speech for First Amendment purposes." That is undoubtedly so. But *Sorrell* involved a statute that prohibited the sale of doctors' prescription-buying preferences to pharmaceutical manufacturers for marketing purposes while allowing the same information to be sold to other users, such as "educational communications," thereby favoring academic research over marketing. The Supreme Court held that the statute impermissibly imposed both content-based and viewpoint-based discrimination and subjected it to the highest level of scrutiny.[24] This bill's changes, by contrast, are neither content- nor viewpoint-based. Thus, that case appears to have little applicability to this bill.

ARGUMENTS IN SUPPORT: Oakland Privacy writes in support:

> Due to the ubiquity of the information state and an advertising ecosystem that has shifted into detailed dossiers for hyper-targeted individualized marketing, the universe of publicly available information is immense. It includes many government records, including professional licensures, property records, court records, census data, voting rolls, public

---

[20] 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.
[21] 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/
[22] Cal. Const. Art. 1, § 3.
[23] (2011) 564 U.S. 552, 570.
[24] *Id.*, p. 565.

records and public meeting minutes, as well as private records including published articles, media interviews, academic conferences and journals, and of course online blogs and social media posts.

Under SB 435, two significant changes would be made to the definition of publicly available information.

Firstly, the phrase "reasonable basis to believe" would be removed from the second bullet point which discusses how a business deals with personal information that is lawfully made available or is in widely distributed media. The default for a business not treating personal information as personal information should be knowledge that it is lawfully available, not beliefs, suppositions or assumptions. If a business lacks knowledge of whether personal information has lawfully been made public, they should not engage in guessing games. They should treat the personal information as personal information, unless and until they have concrete knowledge that the information is public or has been distributed in widely available media. This is a clearer and less ambiguous standard and one that puts safety first.

The second change is the removal of a bullet point about information made available by the consumer if the consumer has not restricted the distribution of the information. This change is responsive to the current realities, where information is widely scraped from digital platforms and it is, at best, unclear what if anything, a consumer can do to prevent that scraping. The clause was written as if privacy control mechanisms were crystal clear and fully transparent to consumers who can clearly indicate exactly what they intend. But our reality, especially online and in the wooly world of social media, is nowhere near that cut and dried. A privacy law intended to be protective of our personal information can not be effective if it places a formidable gauntlet in front of a user/consumer that they must cross in order to receive the protections of the law. And we know that users/consumers that are the most vulnerable are often the ones that are poorly positioned to navigate confusing privacy controls and distribution limits successfully, including young people, the elderly and limited English fluency populations. Reducing the get out of jail free card for what is fundamentally just carelessness and the lack of tech savvy makes us all safer.

These changes meet the standard for amending CPRA by being more privacy-protective than the original language, preserve necessary carve outs for public records and the exercise of journalism, and are responsive to the challenges of the modern day. >

Privacy Rights Clearinghouse also argues in support:

Under current law, the CCPA defines "personal information" as anything that identifies, relates to, describes, or is reasonably capable of being linked to a consumer or household. Depending on how personal information is made available and distributed, and with whom it is shared, those protections are eased and the information is treated as publicly available. Current statute gives businesses significant discretion to interpret any information published online as publicly available. As a result, data brokers can legally access and sell information about where you live, shop, work, study, and travel, along with the status of your reproductive health, marriage, and citizenship, and much more.

When paired with AI tools, this data can build a comprehensive profile of a person's life, allowing agencies to identify, surveil, and track undocumented immigrants and people protesting the federal government with precision. Additionally, this loophole allows

governmental agencies to bypass the Fourth Amendment and increasingly surveil Californians.

SB 435 addresses the loophole in the definition of "publicly available information" by removing language that allows this data to be treated as anything less than sensitive and private by data brokers and corporations. SB 435 does not impact First Amendment protections for information that is truly publicly available; instead, it removes the ability for businesses to overclassify information as publicly available.

ARGUMENTS IN OPPOSITION: In opposition to the bill, [a coalition of business associations] argue:

Ultimately, despite undergoing recent amendments, SB 435 raises largely the same fundamental policy and constitutional concerns presented by last year's version of the bill—concerns that this committee previously considered and rejected.

Even as amended, SB 435 still disrupts careful balance between privacy and the free flow of information

Under the CCPA, "publicly available" includes any of the following: (I) information that is lawfully made available from 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; and (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. (See Civil Code Sec. 1798.140(v)(2)(B).) The definition reflects a recognition in existing law that there are ways for consumers and website operators to restrict access to data via audience controls or similar mechanisms, ensuring that the information would not be considered publicly available. Similarly, there are considerations that go into deciding whether records, or portions of government records should be made publicly available for purposes of the California Public Records Act. (See Gov. Code Sec. 7920.000 et seq.). SB 435 would ignore the careful balance struck in the CCPA between consumer privacy and the free flow of information.

The CCPA excluded information that was made publicly available, as defined, from the definition of "PI" both for public policy and constitutionality purposes. A consumer's privacy interest diminishes in information that is lawfully rendered publicly available in government records, mass media, or otherwise made available to the public by the consumer, including where the consumer makes the information available to other people without placing any restrictions on the audience. Conversely, once information has lawfully entered the public sphere, the public's interest in receiving, accessing, and using that information increases. Again, as noted above, recognizing that there are mechanisms by which a consumer could have ensured that information did not enter the public sphere, once that information does enter that space, Article 1, Section 3 of the California Constitution, California Public Records Act, and the First Amendment of the U.S. Constitution protect the public's access to public information.

Fifty-five years after the Supreme Court expressly recognized the "right to receive information and ideas", it is troubling to see proposals continue to challenge these same foundational principles. It is worth noting that the public's right to receive lawfully available information does not depend on whether that information is generic or specific, fiction or

non-fiction, personal or impersonal, political or apolitical, conservative or liberal, on a particular topic or topics, or of one viewpoint or another. Once information has been lawfully made public, it can — and must — remain available to Californians, including businesses, subject to established limits.

Of course, that is not to say that the Public Records Act, or even the First Amendment or Article 1, Section 3 of the U.S. and California constitutions are without limit—no constitutional or statutory right is, as rights often compete against one another. Indeed, all three of these laws incorporate some version of a balancing test. Likewise, the CCPA's "publicly available" exemption already provides guardrails.

For example, for a record to be "lawfully made available through government records" prong of the "publicly available" exemption, sensitive identifiers will have to have been redacted to protect privacy before release. That is because the Public Records Act in fact demands that privacy interests in public records be weighted against the public interests in the disclosure of those same records under a balancing test that is used to determine whether or not an agency should withhold (or redact) records. This is in addition to a multitude of specific exemptions provided under the act. (Gov. Code Sec. 7927.500.)

Similarly, the second prong of the CCPA's "publicly available" exemption reflects a practical and well-calibrated balance, recognizing that businesses are not always in a position to determine with complete certainty how information came to be publicly available or investigate the circumstances surrounding every public disclosure years after the fact. Accordingly, the statute does not mandate perfect knowledge. Instead, it requires that the business have a reasonable belief that the information was lawfully made available to the public. SB 435 overrides these tested and balanced frameworks, replacing the CCPA's objective reasonable-belief standard with a de facto strict-liability regime based on facts outside a business's knowledge or control at the time it collects, uses, or disseminates information.

Now, information that a business reasonable believes was lawfully disclosed could later be deemed "nonpublic" if it is discovered that the information originated from a record that was improperly released or insufficiently redacted, even where the business had no reason to know of the defect. The bill thus transforms a workable, objective standard into one that depends on facts outside a business's knowledge or control.

Similarly, by deleting the third prong of the publicly available exemption, SB 435 eliminates protection for information that enters the public sphere through third parties to whom the consumer voluntarily disclosed the information without audience restrictions. This includes information publicly shared or republished by others after a consumer chose not to limit its dissemination could be treated as PI notwithstanding its longstanding public availability. For example, information provided by an individual to a professional association for inclusion in a public member directory or to an event organizer for inclusion in a publicly available speaker list could lose its status as "publicly available" despite the individual's decision not to restrict further dissemination. In doing so, the bill disregards the very distinction the CCPA draws between information intentionally made available to the public and information that consumers choose to keep private.

Nothing in SB 435 explains why this longstanding framework should be discarded, particularly where existing law already incorporates multiple safeguards to protect privacy

interests before information enters the public sphere. Nonetheless, these changes upend the voter-approved balancing of interests reflected in Proposition 24, when they not only affirmed but broadened the CCPA's definition of what is considered "publicly available," and therefore exempt from the CCPA , and threaten the substantial societal benefits of protecting access to publicly available information. And the ramifications of doing so would be significant for our members not merely in terms of infringing upon their rights, but from a business and compliance standpoint.

Even as amended, SB 435 still significantly disrupts existing CCPA compliance frameworks

While the bill proposes a seemingly simple change, it would directly and significantly impact our associations and members, who have spent years and significant amounts of resources designing and building their compliance processes to accurately and effectively distinguish between "publicly available" information and "PI" (which includes "sensitive PI") under the CCPA, for the purposes of restricting the sale or sharing of information, as well as limiting the use and disclosure of sensitive PI, and to effectuate other rights afforded by the CCPA. By upsetting this careful balance between privacy and publicly available information, the bill would undermine companies' ability to comply with the CCPA and fulfill consumer rights.

Ultimately, however well-intentioned and compelling it may be in light of recent events, the State may not infringe upon these rights to protect a generalized interest in consumer privacy and such broad-brush restrictions on the collection and dissemination of publicly available information do not appear to be narrowly tailored to further compelling governmental interests as the bill is currently drafted. As a result, the bill seems unlikely to survive strict scrutiny if so challenged.

Lastly, we 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 re-classified "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.

The opposition notes that their arguments against the prior version of SB 435 remain unchanged in this version of SB 435. For an analysis of those arguments please see the 6-23-2025 analysis of this bill, beginning on page 11.

REGISTERED SUPPORT / OPPOSITION:

Support

Alliance for a Better Community (UNREG)
Alliance for Boys and Men of Color
Alliance for Children's Rights

Asian Americans Advancing Justice Southern California
California State Pta
California Teachers Association
Children's Advocacy Institute
Consumer Reports
Consumer Watchdog
Courage California
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice
Seiu California
Unidosus
University of California Student Association

Opposition

Association of National Advertisers
California Chamber of Commerce
Computer & 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 / P. & C.P. / (916) 319-2200