Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1542 (Ward) – As Introduced January 5, 2026

SUBJECT: Sensitive personal information

SYNOPSIS

Americans leave a trail of personal data with almost every action they take either in the physical world or online, including every website visited, credit card payment, and browser search. For almost two decades, experts have been warning about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed.

Surveillance capitalism brings with it a myriad of potential harms. It creates dossiers that can easily reveal a person's reproductive health needs and choices, a person's gender and whether they are seeking gender affirming care, and a person's country of origin and immigration status. In the current political environment, these dossiers can easily cause someone to be imprisoned or killed. This bill intends to limit the circulation of some of the most intimate and sensitive information.

In 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which amended the California Consumer Privacy Act (CCPA) to provide additional privacy rights for consumers and create a new agency charged with enforcing the CCPA. A significant difference between the CCPA and the CPRA was the concept that some personal information was more sensitive than other personal information and was therefore deserving of additional protection. The list of sensitive information includes precise geolocation, ethnicity, immigration status, and the contents of emails and messages, among others.

While sensitive information was determined by the proponents of the proposition to be important enough to be distinguished from other personal information, the proposition did not include robust additional protections. Consumers are still required to opt out of the selling and sharing of their sensitive information, just as they do for all personal information. The primary distinction between the protection for all personal information and for sensitive information is that consumers can limit a business's use *of sensitive personal information.*

The bill amends further amends the CCPA to ban the sale and sharing of sensitive personal information, including but not limited to a consumer's social security number, financial account information, precise geo-location, racial or ethnic origin, religious or philosophical beliefs, union membership, genetic data, biometric information, health information, sexual orientation or citizenship and immigration status.

This bill is sponsored by Consumer Reports, the California Initiative for Technology and Democracy (CITED), and Asian Americans Advancing Justice SoCal and enjoys the support of approximately three dozen privacy and social justice organizations. It is opposed by just over a

dozen business organizations including a coalition of four advertising associations, the California Chamber of Commerce, and TechNet.

EXISTING LAW:

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

2) 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.)

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

4) 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:

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.

c) "Sell," "selling," "sale," or "sold,'' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

i) For purposes of this title, a business does not sell personal information when:

(1) A consumer uses or directs the business to intentionally:

(a) Disclose personal information.

(b) Interact with one or more third parties.

d) "Sensitive personal information" means personal information that reveals a person's:

i) Social security, driver's license, state identification card, or passport number.

ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

iii) Precise geolocation.

iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

viii) Information concerning sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

e) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and

a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

i) For purposes of this CCPA, a business does not share personal information when:

(1) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(2) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purpose of alerting a third party that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(3) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, if information is used or shared consistently with this title, as specified.

5) States that biometric information collected by a business about a consumer without the consumer's knowledge is not considered "publicly available.".

6) Excludes publicly available information from being considered personal information or sensitive personal information.

7) 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).)

8) 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 § 1798.12.)

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.)

9) In the case of sensitive personal information, provides consumers with the additional right to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's 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).)

a) Once a business has received direction from a consumer not to use or disclose the consumer's sensitive personal information, it is prohibited from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction. (Civ. Code § 1798.121 (b).)

b) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section and shall be treated as personal information. (Civ. Code § 1798.121 (d).)

10) 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).)

11) 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.)

THIS BILL: Prohibits a business from selling or sharing a consumer's sensitive personal information.

COMMENTS:

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

With the rapid growth of the data broker industry, tech companies are quietly harvesting and selling detailed information about where people go—from protests and political gatherings to reproductive health clinics, places of worship, and shelters. Recent reports have revealed that federal agencies, including ICE, have purchased this data to conduct surveillance and detain individuals—sidestepping legal safeguards and public accountability.

Californians should not have to worry that their sensitive personal information is being sold to the highest bidder. From precise location data to deeply personal information, AB 1542 draws a clear line—it puts the safety and privacy of everyday Californians first.

2) **Californians' right to privacy**. In 1972, at the Legislature's urging, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution.[1] 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. . . ."[2]

In 2018, the Legislature enacted the California Consumer Privacy Act (CCPA) (AB 375 (Chau, Ch. 55, Stats. 2018)), which gave consumers certain rights regarding their personal information,[3] 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.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which expanded privacy rights for Californians and also reduced privacy protection through the expansion of what would be considered "publicly available information". A significant difference between the CCPA and the CPRA was the concept that some personal information was more sensitive than other personal information and was therefore deserving of additional protection. The list of sensitive information includes precise geolocation, ethnicity, immigration status, and the contents of emails and messages, among others.[4]

While sensitive information was determined by the proponents of the proposition to be important enough to warrant additional layers of privacy, the proposition did not include robust additional protections. Consumers are still required to opt out of the selling and sharing of their sensitive information, just as they do for all personal information. The primary distinction between the protection for all personal information and for sensitive information is that consumers can limit a business's use of sensitive personal information.[5]

With the passage of the CCPA and the CPRA, California, at the time, had the most comprehensive laws in the country when it came to protecting consumers' rights to privacy.

3) **Other states.** Since the passage of the CCPA, 19 additional states have passed comprehensive privacy laws, and 16 additional states currently have active bills in their legislatures. Of the 19 states with laws, 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.[6] Similarly, in 2025, Oregon passed legislation that prohibits businesses from processing personal data for the purposes of targeted advertising, or selling personal data that accurately identifies within a radius of 1,750 feet a consumer's present

---

[1] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[2] *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.
[3] Civ. Code § 1798.140(v). See **EXISTING LAW** #10(a) for definition.
[4] See **EXISTING LAW** section (4)(c)
[5] Civ. Code § 1798.140(ae).
[6] *US State Privacy Legislation Tracker 2026: Comprehensive Consumer Privacy Bills*, International Association of Privacy Professionals (last updated Mar. 23, 2026). https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt76d030a1054f612a/us_state_privacy_legislation_tracker.pdf

or past location or the present or past location of a device that links or is linkable to the consumer.[7]

In the states that have come after California, privacy is the default. The CCPA, on the other hand, 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 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 often 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.

4) **Tracking our every move.** Data and personal information are the new extractive commodities of the age. Often compared to oil, data may be a more renewable resource, albeit at a cost to privacy, autonomy, democratic accountability, consumer choice, and indeed, the environment (in the form of massive energy costs for data centers, e-waste, and the mining of rare minerals).[8]

Americans leave a trail of personal data with almost every action they take either in the physical world or online, including every website visited, credit card payment, and browser search.[9] This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist Shoshana Zuboff. Essentially, surveillance capitalism is an economic system built on the secret extraction and manipulation of human data.[10] In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .
>
> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[11]

With the rapid growth in the development of Artificial Intelligence (AI) systems, particularly large-language models, personal information has become increasingly valuable as developers require ever-growing amounts of data to train their foundation models. Going forward, AI

---

[7] Oregon House Bill 2008 (2025). https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB2008.
[8] https://irisnrc.wisc.edu/wp-content/uploads/sites/1577/2021/06/Privacy-under-Surveillance-Capitalism.pdf.
[9] Emile Ayoub and Elizabeth Goitein. *Closing the Data Broker Loophole*, The Brennan Center for Justice (Feb. 13, 2024).
[10] Zuboff, Shoshana, "You are the Object of a Secret Extraction Operation," *New York Times* (Nov. 12, 2021). https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[11] *Ibid.*

development will continue to increase developers' hunger for training data, fueling an even greater race for data acquisition than we have already seen in past decades.[12]

A 2023 investigation by Consumer Reports on the surveillance economy looked at the companies that share people's personal information with Facebook. Consumer Reports explains:

> One way to understand [the surveillance economy] is as the subset of consumer marketing in which the data being used is obtained from the surveillance, or covert observation, of ordinary consumer activities such as visiting websites, buying goods or services from an online or physical retailer, using one's credit card, and consuming entertainment content.
>
> The surveillance economy is "cross-contextual," meaning that it uses information about individuals that's been collected in one context—such as a website visit, an action taken in an app, or a visit to a physical location—and applies it to another context to affect how you are advertised to, what prices you see, and how you are otherwise treated.[13]

The study's findings reveal that 709 of their participants had their personal information shared by a total of 186,892 companies. On average, each participant was represented in data shared by 2,230 different companies and some were represented in data shared by over 7,000 companies.[14]

These data points will likely be copied millions of times by various algorithms designed to send advertisements and then added to huge databases that enable marketers to create differing scenarios and outcomes to predict your behavior and your interests. Staggeringly, 2.5 quintillion bytes of data are generated every day (that's 18 zeros). That number will continue to grow. Search engines alone log around 6.4 billion searches per day.[15]

Surveillance capitalism brings with it a myriad of potential harms. It creates dossiers that can reveal a person's reproductive health needs and choices, a person's gender and whether they are seeking gender affirming care, and a person's country of origin and immigration status. In the current political environment, these dossiers can easily cause someone to be imprisoned or killed. Sensitive personal information and the inferences that can be made using the information can also have profound and dire consequences for those women who find themselves in an abusive relationship.

During a recent Committee informational hearing on mass surveillance, Professor Ari Ezra Waldman detailed the dangers of this mass data extraction and the extensive dossiers:

> The harms of this kind of data extraction may seem obvious, but allow me to highlight a few of them nonetheless. Data extraction driven by a pathological demand for engagement strips us of our autonomy. It treats us as merely means to someone else's end. It reduces us to numbers and metrics that see humans as merely fitting into categories like Romance Novel

---

[12] King, Jennifer and Meinhardt, Caroline. *Rethinking Privacy in the AI Era*. Human-Cantered Artificial Intelligence at Stanford University (Feb. 2024) https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

[13] 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/

[14] *Ibid.*

[15] Ebsworth, Jonathan, et al. *Surveillance capitalism: the hidden costs of the digital revolution* (2021).

> Reading Urbanites or Christian Serial Daters or Susceptible to Splurge Purchases, all of which are real categories. These harms metastasize for the most marginalized among us, who are already told by society that they are less than or less deserving of protection. We see it everyday: the deaths by suicide, the harassment, the microtargeting, the misinformation, and other real social harms.
>
> Some people, often those more technically inclined or those who trust technology to solve social problems for us, may tell you that the answer to the harms of data collection is actually to collect more data. To stop discrimination and harm, companies need more information about who we are and what is happening to us. In the AI context, computer scientists call this "fairness through awareness". The best way to stop disparate impact from AI systems is to let the AI take diversity into account.
>
> Don't be fooled by this argument. It is a smokescreen to continue rampant, unregulated data collection on the backs of those who, sometimes, don't want the information collected in the first place. Why would those most susceptible to the harms of surveillance want private or public entities to surveil them more to make their products more accurate at surveillance? It just doesn't make sense.

5) **Notice and consent.** Opponents of the bill, a coalition of organizations representing the advertising industry, argue that "The CCPA already requires transparency and consumer choice: businesses must provide consumers with a notice at collection describing the categories of sensitive personal information collected and the purposes for its use, must disclose consumers' rights in privacy policies, and must give consumers a right to limit the use and disclosure of sensitive personal information when it is used beyond narrow statutorily defined purposes. Current law gives consumers the right to *decide* whether data can be used and allows them to *choose* whether to receive the benefits that come from its use. AB 1542 would take that choice away from consumers."

In addition, a coalition of business organizations including the California Chamber of Commerce, asserts:

> Recognizing the vast amount of personal information in the hands of businesses, the CCPA was intentionally designed to give consumers greater control over their data, applying broadly to online companies, brick and mortar stores, the tech industry or any number of other industries. It was further designed to apply to some businesses based on their annual gross revenue, and others based on their data practices. Across all of these, consumers were to be given the same rights over all their personal information—whether that information was a drivers' license number, their name, their purchase history, their location data, or account info, or other forms of data. Balancing was done over when notices should be given, when there should be an opt-out versus an opt-in, with considerations over things like notice/consent fatigue, but always the point was to put power in the hands of the consumer. Even for teenagers, it was recognized that it was their data, and not the data of their parents and so at certain ages, the decisions belonged to them to make on their own behalf, consistent with other California laws recognizing rights of minors, such as in the medical privacy space.
>
> [. . .]

> This bill would for the first time since 2018 take away that control from consumers, abandoning any opt-out or opt-in rights altogether in favor of a complete ban on selling or sharing data with third parties, cutting off access to certain information to businesses and consumers entirely.

The opposition is correct: the general framework for California's privacy laws focus on the rights of the individual and the idea that personal information can be collected, used, sold and shared if the person grants informed consent – either by opting out of the sharing or opting into the sharing. This presumes that visitors to a website will read the policies and determine whether they are comfortable with the way that their personal information will be used and collected. It also presumes that they will be able to determine which businesses have their data in order exercise their rights under the CCPA.

On this issue of the notice and consent model, Professor Waldman notes, "Legislators in the United States believe they have found the perfect recipe for privacy law: individual rights of control."[16] In most states that have privacy laws, policymakers are proposing and enacting privacy laws that give us some combination of the right to access the information companies have on us, delete it if we want, correct it if there are mistakes, and move it to another company. California is especially prone to this model of privacy protection.

Nicole Ozer, in her paper *Putting People Power into US Privacy Law* summarizes the general thinking on the value of notice and consent this way:

> It is recognized that "consent in privacy is beyond broken, it is a complete fiction." The notice and consent regime is plagued with challenges and invites "unwitting and coerced consent." People care about protecting their privacy but can often be "nudged and manipulated by powerful companies against their actual interests," with consent "deployed in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power."[17] [Citations omitted]

During this Committee's recent informational hearing on mass surveillance, Professor Dierdre Mulligan framed it this way:

> Existing privacy laws built around notice and consent, assume individuals are aware of and have a say over the collection of their personal data. The infrastructuring of physical spaces has pushed data collection behind the scenes and often outside of individuals' control. A person's presence in a physical space–a workplace, a public street, a commercial store–routinely subjects them to surveillance often without their knowledge and almost always without meaningful consent. In personal homes and on public streets, the Internet of Other people's things extract data from individuals based on other people's preferences. Surveillance has become the background condition of everyday life rather than an episodic event brought to an individual's attention and over which they might be afforded some control.

---

[16] Ari Ezra Waldman, *Privacy's Rights Trap,* Northwestern University of Law Review (2022).
[17] Nicole A. Ozer, *Putting People Power into US Privacy Law: Learning from the Past to Light the Path to True Privacy Protection to Advance Rights and Democracy in the Age of Artificial Intelligence*, Harvard Kennedy School's Carr-Ryan Center for Human Rights (Fall 2025).

> Existing privacy laws, built around notice and consent at the moment of data collection, assume individuals understand the risks posed by disclosing different kinds of personal information because they understand what it reveals about them–i.e. they assume individuals understand the meaning of their data. In other words, privacy laws in the United States generally assume that the semantics of data are relatively fixed and knowable at the time of disclosure. But armed with sophisticated and powerful machine learning algorithms, companies (and governments) can draw powerful and compromising inferences from seemingly benign data making it increasingly difficult for individuals to understand the meaning, let alone the risks of disclosing any piece of their data. In this asymmetric environment, individuals' ability to control who knows what about them cannot be fully protected by notice and consent mechanisms focused on data collection.[18]

6) **Analysis.** One could argue that the State's current consumer privacy laws 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 the proposition promised that adding a 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."[19] In 2026, a person would be hard-pressed to find that level of privacy in their homes, much less outside of those formerly private spheres.

As discussed previously, while the proponents of Proposition 24 decided that certain personal information should be distinguished as sensitive information and provided with additional protections, unfortunately they failed to provide robust protection. Fortunately, the proponents of the CPRA and the voters in 2020 understood that the Legislature may need to move beyond the CCPA to continue to protect Californian's right to privacy. They understood that the CCPA was a floor and not a ceiling. This bill is in keeping with that premise by strictly prohibiting the sharing and sale of data that has been designated as sensitive because of its potential to reveal our most sensitive and intimate information.

Concern raised by the opposition. The coalition of business interests, including the California Chamber of Commerce and TechNet, argue that this bill could have unintended consequences by prohibiting the sharing of sensitive information. Among the consequences they cite are the following:

1. Fraud prevention tools often rely on signals observed across multiple merchants to detect coordinated attacks and prevent account takeovers.

2. Location-based services depend on third party data inputs to provide accurate, real-time navigation.

3. Emergency or disaster-response efforts may rely on aggregated mobility data to allocate resources efficiently.

---

[18] *Testimony of UC Berkeley Professor Deirdre Mulligan Before the California Assembly Committee on Privacy and Consumer Protection* (Mar. 3, 2026) https://apcp.assembly.ca.gov/system/files/2026-03/deirdre-mulligan-surveillance-capitalism-testimony-03-03-2026.pdf.

[19] *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..

4. Organizations responding to disasters or coordinating relief efforts often rely on sensitive PI, such as geolocation or household data to allocate resources efficiently and reach those in need.

However, the definition of "sharing" in the CCPA[20] narrowly applies to the provision of personal information to a third party for *cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.* The restrictions in the bill, therefore, apply only to the sharing of sensitive information in order to target users with personalized ads based on their activity across multiple websites, apps, or services. Consequently, the information-sharing purposes outlined by the opposition would be unaffected by this bill.

More work to be done. Oakland Privacy, writing in general support of this bill, raises the following concerns about the constraints of the CCPA and the work that remains to be done:

> [T]he two-tiered consent structure [related to personal information and sensitive personal information] has certainly proven to be a bit clunky. Users have reported significant difficulty understanding complex cookie menus. And follow-up legislation including AB 566 (Browser Global Opt Out) and SB 362 (Delete Act) have followed the CPRA to try to make it easier for Californians to actually control private sector use of their personal information. What this tells us is that privacy controls are continuing to evolve as data marketplaces grow ever more complicated and convoluted. In other words, we aren't done yet.
>
> AB 1542 generally posits that data marketplaces, of all kinds, should not traffic in sensitive personal information. Its guiding principle is that consumers disclose this information to companies only for first-hand and direct purposes and with only narrow exemptions, not for general circulation or collateral profit-making activities. Oakland Privacy believes this is consistent with the wishes of the majority of Californians, whether or not they have the time, willingness or technical aptitude for negotiating those complex cookie menus. Numerous polls and surveys back up this belief.
>
> So AB 1542 prohibits the sale or sharing of any Californians sensitive personal information to any third party, regardless of a consumer consenting or not consenting. This forcibly limits the data broker marketplace to selling information obtainable from public records or non-sensitive personal information. This restricts the behavioral advertising ecosystem to using only non-sensitive data (i.e. one's taste in hats or airlines, not one's sexual orientation or precise location). This will significantly reduce the identity theft scourge by reducing the commercial circulation of social security numbers, drivers' licenses and log-in credentials. These are all objectively well-aligned with the privacy concerns that Californians most frequently express.
>
> It's important to recognize that AB 1542 operates within the context of California's existing CCPA/CPRA comprehensive privacy laws. Covered entities under the law would remain the same: companies with tens of millions in revenue or more, or companies that handle large quantities of personal information. The exemptions in CPRA, which are somewhat extensive, would also apply under AB 1542. These include exemptions for law enforcement and

---

[20] See **EXISTING LAW** 4) e).

regulatory investigations, court orders and subpoenas, immediate risk of serious injury, medical research, job application and benefits processing, and credit marketplaces. Direct service providers and contractors to a business are also exempt from the definition of a third party to continue to facilitate loyalty programs and other discount programs.

ARGUMENTS IN SUPPORT: California Initiative for Technology and Democracy (CITED), co-sponsors of the bill, write in support:

Privacy is the backbone of a democratic society, enabling people to gather, voice their opinions, and perform lawful action without fear of surveillance or retribution. The state recognized this essential and inalienable right in 1972 when the voters of California inscribed privacy into our State's Constitution, with the encouragement of the Legislature. In arguing for the proposed constitutional amendment, proponents stated:

> "Computerization of records makes it possible to create 'cradle-to-grave' profiles on every American […] 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 or to embarrass us."

The collection of mass amounts of information is not solely a practice of the private sector. Local, state, and federal governments can easily access this information through data brokers and begin to build personal dossiers on individuals, circumventing our Fourth Amendment rights. At a moment when California faces challenges from a punitive federal administration, it is of the utmost importance that our state protect our communities. It has already been well established that data brokers can identify individuals who engage in civil action, such as those who attend protests, raising concerns about how one can move or act freely when the federal government seeks to limit such activities. California cannot allow its data infrastructure to become a tool of federal overreach. AB 1542 is a necessary step toward ensuring that the sensitive personal information of our residents cannot be weaponized against the very communities our state has pledged to protect.

AB 1542 would ban the selling and sharing of sensitive personal information. Sensitive personal information as defined in the California Consumer Privacy Act (CCPA) includes a consumer's government identifier (Social Security, driver's license, passport numbers); financial account credentials; precise geolocation; racial or ethnic origin, citizenship or immigration status, religious beliefs, or union membership; the contents of private communications; and genetic, neural, and biometric data. It also includes personal information concerning a consumer's health, sex life, or sexual orientation.

Currently, the CCPA gives consumers the right to opt out of or limit the use and disclosure of their sensitive personal information. While this is a well-meaning measure, it fails to provide sufficient protection. A 2023 Consumer Reports study found that among 709 participants, each person's data had been shared by an average of 2,230 companies, with some by over 7,000.4 California's Delete Act is a meaningful step forward, but it is simply not realistic to expect consumers to track where their information is being collected and shared, let alone control that flow. A true prohibition on the selling and sharing of sensitive personal information is the only way to ensure that protection does not depend on a consumer's awareness, resources, or ability to navigate an overwhelming and opaque data marketplace.

In addition, a coalition of privacy rights organizations notes:

> Sensitive personal information reveals the most intimate parts of ourselves, including our immigration status, sexual orientation, location, political activities, genetic and health information, and even the contents of our communications. This type of data has been used by scammers to facilitate financial fraud, by retailers to generate predatory pricing schemes, and even by our own federal government to surveil individuals exercising their constitutional rights. It is imperative we protect the privacy rights of our communities, especially with increased attacks on immigrants, Black and Brown community members, LGBTQ people, and individuals seeking reproductive health care. California must take bold action to ensure individuals are protected and their sensitive personal information is kept private. AB 1542 answers this call.
>
> Many of our privacy laws revolve around an opt-in/out model. Unfortunately, such consent processes typically do not provide an explanation about who will receive consumers' sensitive personal information or how it will be used. And often, consumers are forced to opt-in just to access the underlying product or service they want. Ultimately, consumers are inundated with so many consent requests that they have lost their meaning. We need a better way.
>
> While there are plenty of reasons why consumers allow businesses to collect their sensitive data (e.g. to provide turn-by-turn directions or provide personalized health recommendations) this information should never then be sold to third-parties for unrelated purposes. Unfortunately, this is often what happens today, and once our information is shared or sold, it is impossible to claw it back. AB 1542 addresses this problem by ensuring that our sensitive personal information will stay with the business we have initially provided it to and will not be sold to the highest bidder.

ARGUMENTS IN OPPOSITION: In opposition to the bill, the California Chamber of Commerce along with others in a business coalition argues:

> The California Chamber of Commerce and the undersigned respectfully OPPOSE AB 1542 (Ward) as introduced January 5, 2026, because it bans the selling and sharing of sensitive personal information by certain businesses and fails to recognize any legitimate purposes for which an entity covered under the California Consumer Privacy Act (CCPA) should be permitted to disclose sensitive personal information (SPI), even with the consumer's permission. This could result in a host of unintended consequences, including ones that have serious safety implications, such as prohibiting a business from transmitting precise geolocation data in the event of a car crash, even if a customer would have allowed them to do so if asked. In particular, such a categorical prohibition risks sweeping in routine and lawful data-sharing practices that underpin modern internet operations, including cloud storage, basic website functionality, security and fraud-prevention activities, and processing under data-processing agreements. In doing so, the bill could not only make it more difficult to prevent fraud, but it could also interfere with the ability of businesses to complete transactions.
>
> And because of the range of data included under SPI, AB 1542 can also significantly impede the ability of California businesses in arguably "sensitive" sectors to advertise and reach consumers online—the impact of which would be particularly damaging for small and medium businesses, which generally do not have large ad budgets and rely on cost-effective

targeted online advertising. For consumers, this means that they would not see as relevant or helpful ads, losing access to the goods and services that they are most likely to find useful or beneficial, including those that they might not otherwise become aware of on their own. Community groups and organizations focused on health and social issues, and political organizations who purchase data from covered businesses may also see a decrease in effectiveness of ads – ultimately interfering with the ability of Californians to connect to the resources they need and political parties from connecting with their voter base.

REGISTERED SUPPORT / OPPOSITION:

Support

Asian Americans Advancing Justice Southern California (Co-Sponsor)
California Initiative for Technology & Democracy, a Project of California Common CAUSE (Co-Sponsor)
Consumer Reports (Co-Sponsor)
A Voice for Choice Advocacy
Aapis for Civic Empowerment
California Coalition for Worker Power
California Domestic Workers Coalition
California Federation of Labor Unions
California Health Coalition Advocacy
California Immigrant Policy Center
California Work & Family Coalition
Calpirg, California Public Interest Research Group
Chinese Progressive Association
Consumer Attorneys of California
Courage California
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
End Child Poverty California Powered by Grace
Equal Rights Advocates
Equality California
Indivisible Ca: Statestrong
Kapor Center Advocacy
Lgbt Tech
Oakland Privacy
Pilipino Workers Center
Privacy Defense Alliance
Privacy Rights Clearinghouse
Reproductive Freedom for All
Secure Justice
Seiu California
Southeast Asia Resource Action Center (SEARAC)
Techequity Action
Ultraviolet Action
Warehouse Worker Resource Center
Western Center on Law & Poverty
Women's Foundation California

Opposition

American Advertising Federation (AAF)
American Association of Advertising Agencies (4A's)
American Property Casualty Insurance Association
Association of National Advertisers
California Chamber of Commerce
California Retailers Association
California's Credit Unions
Civil Justice Association of California (CJAC)
Computer and Communications Industry Association
Digital Advertising Alliance
Insights Association
Internet.works
Software Information Industry Association
Technet

Oppose Unless Amended

Ata Action
California Asian Pacific Chamber of Commerce
Inmarket Media, LLC
Network Advertising Initiative

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