SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 1542 (Ward)
Version: January 5, 2026
Hearing Date: June 22, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Sensitive personal information

DIGEST

This bill prohibits the selling or sharing of "sensitive personal information" pursuant to the California Consumer Privacy Act (CCPA).

EXECUTIVE SUMMARY

The CCPA grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. (Civ. Code § 1798.100 et seq.) It places attendant obligations on businesses to respect those rights. Through Proposition 24, California established the California Privacy Rights Act of 2020 (CPRA). The CPRA amends the CCPA, limits further amendment, and creates the California Privacy Protection Agency (CalPrivacy).

The CPRA also created a new category of "sensitive personal information" and afforded consumers enhanced rights with respect to that information, including the ability to restrict businesses' use and disclosure of that information. This category includes data such as precise geolocation information and immigration status.

Given the heightened sensitivity of this information and the widespread weaponization and commodification of it, this bill prohibits the selling or sharing of sensitive information by a business, service provider, or contractor to a third party.

The bill is sponsored by Consumer Reports and the California Initiative for Technology & Democracy (CITED). The bill is supported by many privacy, consumer, labor, and other advocacy organizations, including Equality California and the California Federation of Labor Unions. The bill is opposed by industry associations, including the Association of National Advertisers and ATA Action.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale or sharing of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

2) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer specified information, including the business or commercial purpose for collecting, sharing, or selling personal information and the categories of third parties with whom the business discloses personal information. (Civ. Code § 1798.110.)

3) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of the sale or sharing of their personal information. (Civ. Code § 1798.120.)

4) Defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including identifiers, biometric information, and geolocation data. (Civ. Code § 1798.140(v).) The CCPA defines and provides additional protections for sensitive personal information, as defined, that reveals specified personal information about consumers, including precise geolocation, genetic data, and immigration status. (Civ. Code § 1798.140(ae).)

5) Requires businesses that collect consumers' sensitive personal information to inform consumers of the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. (Civ. Code § 1798.100(a)(2).)

6) Affords consumers the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information, as specified. A business that has received such direction shall be prohibited from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt

of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes. Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject hereto and shall be treated as personal information for purposes of all other sections of the CCPA. (Civ. Code § 1798.121.)

7) Establishes the CPRA, which amends the CCPA and creates CalPrivacy, which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

8) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor, provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

9) Provides that a business need not comply with the CCPA to the extent it restricts the business's ability to carry out certain conduct, including complying with federal, state, or local laws or to cooperate with law enforcement. (Civ. Code § 1798.145(a).)

This bill prohibits a business, service provider, or contractor from selling or sharing the sensitive personal information of a consumer to a third party.

COMMENTS

1. California's landmark privacy protection law

As stated, the CCPA grants consumers certain rights with regard to their personal information, as defined. With passage of the CPRA in 2020, the CCPA got an overhaul. Consumers are afforded the right to receive notice from businesses at the point of collection of personal information and the right to access that information at any time. The CCPA also grants a consumer the right to request that a business delete any personal information about the consumer the business has collected from the consumer. However, a business is not required to comply with such a request to delete if it is necessary for the business to maintain the consumer's personal information in order to carry out certain obligations or other conduct. (Civ. Code § 1798.105(d).)

The CCPA provides adult consumers the right, at any time, "to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out." Changes made by the CPRA extend this to opting out of the "sharing" of the personal information as well. A business is thereafter prohibited from selling (or sharing) that

information unless consent is subsequently provided. A business that sells personal information to third parties is required to notify consumers that this information may be sold and that they have the right to opt out of such sales. (Civ. Code § 1798.120(a).) The CPRA also added a new category of information, sensitive personal information, which includes information that reveals certain data, such as precise geolocation and genetic information. Consumers are additionally empowered to limit businesses' use of such information.

2. Putting our most intimate data up for sale

The mass collection of consumer data as an asset is not new, but has rapidly expanded beyond just targeted advertising. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff:

> 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.[1]

Companies gather data through multiple channels, including purchase history, browsing behavior, location tracking, demographic information, social media activity, and even biometric data. This information gets fed into sophisticated algorithms that create detailed consumer profiles. With the rise of data brokers, the concerns are only further exacerbated:

> Data brokers operate within a multibillion-dollar industry built on the collection and sale of detailed personal information—often without individuals' knowledge or consent. These companies create extensive profiles on nearly every American, including highly sensitive data such as precise location history, political affiliations, and religious beliefs. This

[1] Zuboff, Shoshana, *You Are the Object of a Secret Extraction Operation* (November 12, 2021) The New York Times, https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html. All internet citations are current as of May 31, 2026.

> information is frequently resold for purposes ranging from marketing to law enforcement surveillance.
>
> Many people are unaware that data brokers even exist, let alone that their personal information is being traded.[2]

These concerns are heightened when the underlying information is incredibly sensitive, including information about consumers' exact location, their immigration status, and personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation. These are all considered "sensitive personal information" under the CCPA, but the law does not prevent the selling or sharing of such data. Proponents of the bill point out that, especially given the hostile climate at the federal level and in other states for certain communities, more protections are due.

One recent investigation by Consumer Reports (CR) highlighted the collection and sharing of sensitive health data by private companies, including pregnancy status:

> A recent CR investigation shows that companies providing on-demand workout and fitness services tend to give themselves permission to collect lots of information about you, including potentially sensitive health data. This might include your heart rate or your weight and how it changes over time. It might even include information about your reproductive health.
>
> The smart-home gym company Tonal, for example, says it may collect data about your pregnancy status. Peloton offers workouts specifically for pregnancy and collects information about any workouts you participate in. (Surveillance of pregnant people has become a concern for many Americans in the wake of state and proposed national measures to restrict abortion access.)
>
> In short, when you use a connected exercise machine or app, the company behind it could be collecting and sharing a lot more than just the length and intensity of your workouts. And because of broad privacy policies, it's hard to know where your data will end up and how it will be used.
> …
> In most cases, your data could be shared with a very extensive group of companies. It includes fraud protection companies, IT and technical support providers, payment processors, analytics providers, advertisers,

[2] Dell Cameron & Dhruv Mehrotra, *CFPB Quietly Kills Rule to Shield Americans From Data Brokers* (May 14, 2025) Wired, https://www.wired.com/story/cfpb-quietly-kills-rule-to-shield-americans-from-data-brokers/.

> marketing and database management firms, law enforcement, and government regulators.
>
> A few privacy policies outline specific reasons why certain outside companies might receive your data. Tempo, for example, partners with a company called Prism Labs, which calculates body composition based on head-to-toe 3D body scans.
>
> In all cases, the privacy policies allow the companies to share your information with at least some other organizations. As the privacy policies of BowFlex and several other companies point out, in certain situations this may be legally considered "selling" your data under the California Consumer Privacy Act or other state privacy laws.[3]

Even car manufacturers have been reported to be collecting and sharing information about consumers' sexual activity:

> Car manufacturers are collecting troves of data on drivers and passengers — some even tracking drivers' sexual activity — according to a new report.
>
> In a review of 25 car brands and 15 car companies published by Mozilla Foundation on Wednesday, researchers found that Japanese car manufacturer Nissan said it could sell information about drivers and passengers' sexual activity, intelligence and health diagnosis to data brokers, law enforcement agencies and other companies. German manufacturer Volkswagen said it could record drivers' voices to profile them for targeted ads.
>
> "The amount of data that these car companies blatantly said that they could collect was shocking," said Jen Caltrider, lead researcher at Mozilla Foundation, the nonprofit owner of the company running the Firefox Browser. "It's like nobody's ever challenged them or asked them questions about privacy, and so they just include everything."[4]

---

[3] Catherine Roberts, *Your Exercise Bike Knows a Lot About You – and It Doesn't Keep Every Secret* (January 14, 2025) Consumer Reports, https://www.consumerreports.org/health/health-privacy/exercise-machine-privacy-a3907557984/.

[4] Clothilde Goujard, *Your car wants to know about your sex life* (September 7, 2023) Politico, https://www.politico.eu/article/car-manufacturer-data-privacy-driver-passenger-sexual-activity-report/.

One "nightmare scenario" reveals how the broader selling and sharing of this information also further exposes the sensitive information from falling into the wrong hands:

> Hackers claim to have compromised Gravy Analytics, the parent company of Venntel which has sold masses of smartphone location data to the U.S. government. The hackers said they have stolen a massive amount of data, including customer lists, information on the broader industry, and even location data harvested from smartphones which show peoples' precise movements, and they are threatening to publish the data publicly.
>
> The news is a crystalizing moment for the location data industry. For years, companies have harvested location information from smartphones, either through ordinary apps or the advertising ecosystem, and then built products based on that data or sold it to others. In many cases, those customers include the U.S. government, with arms of the military, DHS, the IRS, and FBI using it for various purposes. But collecting that data presents an attractive target to hackers.
>
> "A location data broker like Gravy Analytics getting hacked is the nightmare scenario all privacy advocates have feared and warned about. The potential harms for individuals is haunting, and if all the bulk location data of Americans ends up being sold on underground markets, this will create countless deanonymization risks and tracking concerns for high risk individuals and organizations," Zach Edwards, senior threat analyst at cybersecurity firm Silent Push, and who has followed the location data industry closely, told 404 Media. "This may be the first major breach of a bulk location data provider, but it won't be the last."[5]

These concerns even prompted the Consumer Financial Protection Bureau (CFPB) in 2024 to propose a rule to limit the ability of data brokers to sell sensitive information about Americans, including financial data, credit history, and Social Security numbers.[6] The rule, entitled Protecting Americans from Harmful Data Broker Practices, was proposed under former CFPB director (and current Secretary of California's newly formed Business and Consumer Services Agency) Rohit Chopra, who argued the rule was "necessary to combat commercial surveillance practices that 'threaten our personal safety and undermine America's national security.'" However, the proposal was withdrawn under President Trump's director of the CFPB.

---

[5] Joseph Cox, *Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data* (January 7, 2025) 404 Media, https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/.

[6] *See* fn. 3.

However, the issue has not been partisan. Texas Attorney General, and United States Senate candidate, Ken Paxton, has established a privacy enforcement team that has been active in holding private entities accountable for improperly collecting and selling sensitive consumer information, including actions taken against car manufacturers for selling driving data and social media companies for capturing biometric data.[7]

Recently, Maryland passed the Maryland Online Data Privacy Act, which completely prohibits controllers from selling sensitive data. It goes further and, except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains, a controller is prohibited from collecting, processing, or sharing sensitive data concerning a consumer.

3. Protecting consumers' most sensitive information

This bill responds to the privacy concerns raised by outright prohibiting the selling or sharing of sensitive personal information. 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.

4. Stakeholder positions

A coalition of advertising associations in opposition, including the Digital Advertising Alliance, argues:

> AB 1542 would add a new clause to the California Civil Code, Section 1798.121, prohibiting businesses, service providers, or contractors from selling or sharing sensitive personal information to third parties. This approach would go well beyond what is necessary to protect consumers and abandon the approach taken by CCPA, as approved by California

[7] F. Paul Pittman, *Texas Attorney General's Landmark Privacy Lawsuit Signals New Era in Data Privacy Enforcement* (February 3, 2025) White & Case, https://www.whitecase.com/insight-alert/texas-attorney-generals-landmark-privacy-lawsuit-signals-new-era-data-privacy.

> voters via ballot initiative. 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.
>
> Rather than preserving the CCPA's framework of data use limitations, informational disclosures, and consumer controls, AB 1542 would impose a one-size-fits-all prohibition that would limit beneficial practices even where consumers have been fully informed and afforded meaningful choice.

Several industry associations, including the California Chamber of Commerce, similarly focus on consumer choice:

> An opt-in mechanism for selling or sharing to third parties, unlike a ban, would allow businesses to seek express consent from the consumer, while prohibiting them from selling or sharing to third parties unless the consumer consents, leaving control in the hands of the consumer. Many consumers are already familiar and comfortable with this process for precise geolocation, for example -- turning off location services in their phone and setting it to "unless shared" for certain apps, and deciding yes/no when prompted by the app for certain uses. On the apps they have chosen "never", on occasion they may ask for something and get reminded they cannot have a certain functionality or service because of that choice and can easily go back and change their setting to "unless shared" if they wish. This process provides some balance between consumer privacy with business needs.

It should be noted that within the definitions of the CCPA, the law explicitly states that a business does not *sell* personal information when a consumer uses or directs the business to intentionally disclose personal information or interact with one or more third parties.[8] Furthermore, a business does not *share* personal information when a consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.[9] Therefore, should the prohibition in the bill go into effect, consumers

[8] Civ. Code § 1798.140(ad)(2).
[9] Civ. Code § 1798.140(ah)(2).

still retain the ability to direct the business to disclose their personal information to third parties and not violate the prohibition of this bill as it would not be considered selling or sharing the information. To make this clear, the author has agreed to an amendment that cross-references that section of the law.

A broad coalition of organizations, including Equal Rights Advocates, the Electronic Frontier Foundation, and SEIU California, write in strong support:

> 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.

5. <u>Furthering the purpose and intent of the CPRA</u>

Section 25 of the CPRA requires any amendments thereto to be "consistent with and further the purpose and intent of this act as set forth in Section 3." Section 3 declares that "it is the purpose and intent of the people of the State of California to further

protect consumers' rights, including the constitutional right of privacy." It then lays out a series of guiding principles. These include various consumer rights such as:

- consumers should know who is collecting their personal information;
- consumers should have control over how their personal information is used; and
- consumers should benefit from businesses' use of their personal information.

Section 3 also includes a series of responsibilities that businesses should have. These include:

- businesses should specifically and clearly inform consumers about how they use personal information; and
- businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes.

Section 3 also lays out various guiding principles about how the law should be implemented.

This bill provides stronger protections for this incredibly sensitive information. This allows for a fuller realization of the benefits intended by the law. Therefore, as it explicitly states, this bill "furthers the purposes and intent of the California Privacy Rights Act of 2020."

SUPPORT

California Initiative for Technology & Democracy, a Project of California Common CAUSE (co-sponsor)
Consumer Reports (co-sponsor)
AAPIS for Civic Empowerment
Abine, INC. DBA Deleteme
Alliance of Californians for Community Empowerment (ACCE Action)
California Domestic Workers Coalition
California Federation of Labor Unions
California Health Coalition Advocacy
California Immigrant Policy Center
California National Organization for Women
California Privacy Protection Agency
California Work & Family Coalition
CALPIRG
CFT – a Union of Educators & Classified Professionals, Aft, AFL-CIO
Chinese Progressive Association
Consumer Attorneys of California
Courage California
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
End Child Poverty CA

Equal Rights Advocates
Equality California
Greenlining Institute
Indivisible Ca: Statestrong
Jewish California (formerly JPAC)
LGBT Tech
Oakland Privacy
Para Los Ninos
Parent Voices California
Privacy Defense Alliance
Privacy Rights Clearinghouse
PWC
Reproductive Freedom for All
Secure Justice
SEIU California
Southeast Asia Resource Action Center (SEARAC)
Tech Oversight California
TechEqiuty Action
Ultraviolet Action
Warehouse Worker Resource Center
Western Center on Law & Poverty
Women's Foundation California

OPPOSITION

American Property Casualty Insurance Association
Association of National Advertisers
Ata Action
California Chamber of Commerce
California Retailers Association
California's Credit Unions
Civil Justice Association of California (CJAC)
Computer & Communications Industry Association
Inmarket Media, LLC
Insights Association
Internet.works
Network Advertising Initiative
Software Information Industry Association
Technet

RELATED LEGISLATION

AB 2564 (Ward, 2026) prohibits the practice of "surveillance pricing," defined as offering or setting a customized price for a good for a specific consumer or group of

consumers, based, in whole or in part, on personally identifiable information collected through electronic surveillance technology, including personally identifiable information collected through electronic surveillance technology that is gathered, purchased, or otherwise acquired from a third party. It provides exceptions for the offering of discounted pricing, such as through loyalty programs, where certain conditions are met, such as ensuring transparency about the basis for such discounts. AB 2564 is set to be heard in this Committee the same day as this bill.

SB 1223 (Becker, Ch. 887, Stats. 2024) included "neural data," as defined, within the definition of "sensitive personal information" for purposes of the CCPA.

AB 947 (Gabriel, Ch. 551, Stats. 2023) included personal information that reveals a consumer's citizenship or immigration status in the definition of "sensitive personal information" for purposes of the CCPA.

AB 1194 (Wendy Carrillo, Ch. 567. Stats. 2023) provides stronger privacy protections pursuant to the CCPA where the consumer information contains information related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including abortion services.

AB 1546 (Gabriel, 2023) would have extended the statute of limitations for actions brought by the Attorney General to enforce the CCPA to five years after the accrual of the cause of action. AB 1546 was held in the Senate Appropriations Committee.

AB 254 (Bauer-Kahan, Ch. 254, Stats. 2023) includes "reproductive or sexual health application information" in the definition of "medical information" and the businesses that offer reproductive or sexual health digital services to consumers in the definition of a provider of health care for purposes of the Confidentiality of Medical Information Act (CMIA).

AB 2089 (Bauer-Kahan, Ch. 690, Stats. 2022) includes mental health application information in the definition of "medical information" and the businesses that offer mental health digital services to consumers in the definition of a provider of health care for purposes of the CMIA.

AB 694 (Assembly Committee on Privacy and Consumer Protection, Ch. 525, Stats. 2021) made nonsubstantive and conforming changes to the CCPA to clean up the language amended in by the CPRA.

AB 375 (Chau, Ch. 55, Stats. 2018) established the CCPA.

PRIOR VOTES:

Assembly Floor (Ayes 42, Noes 19)

Assembly Appropriations Committee (Ayes 11, Noes 4)
Assembly Privacy and Consumer Protection Committee (Ayes 9, Noes 5)

****