CONCURRENCE IN SENATE AMENDMENTS
AB 1542 (Ward)
As Amended August 21, 2026
Majority vote

SUMMARY

This bill prohibits businesses that are subject to the California Consumer Privacy Act (CCPA) from selling or sharing a consumer's sensitive personal information.

Senate Amendments
Allow a commercial credit reporting agency to sell a consumer's social security number to the extent the commercial credit reporting agency uses that information solely to identify the relationship of a consumer to a business that the consumer owns.

COMMENTS

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 protection. 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 of all personal information and for sensitive information is that consumers can limit a business's use of sensitive personal information.

The bill 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.

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.

Arguments in Support

The California Privacy Protection Agency writes:

> Sensitive personal information can reveal deeply personal insights about individuals and therefore deserves heightened protections. The sale and use of information related to health conditions, race, or immigration status, for example, can lead to discrimination and harassment. Similarly, disclosures of personal identifiers and financial data can cause identity theft and fraud.
>
> These risks are magnified by data brokers that collect, aggregate, and sell highly sensitive data — including health records, financial information, location data, and citizenship data — with minimal oversight or consumer consent. A recent enforcement action by CalPrivacy against a Texas data broker demonstrated how the company sold the names, addresses, phone numbers, and email addresses of millions of people with Alzheimer's disease and other health conditions. The same company bought and sold lists of people based on their age, perceived race (including "Hispanic lists"), and political views. This information can be dangerous when placed in the wrong hands.
>
> Limiting both the sale and sharing of sensitive personal information would provide protection against the significant risks of fraud, discrimination, and extortion. Such a prohibition would ensure that everyone's most personal and sensitive information is automatically protected from widespread circulation, minimizing downstream risks that could arise from sharing, such as risk of data breach and misuse.
>
> Increased protections would also enable California to keep pace with other states. In recent discussions related to federal privacy legislation, California's protections for sensitive data have been characterized as "narrow" in comparison to the opt-in framework used by many other states and some states, like Maryland and New Jersey, already prohibit the sale of sensitive personal information.

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.

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.>

FISCAL COMMENTS

According to the Senate Appropriations Committee:

1) Enforcement costs of $536,000 in FY 2026-27 and $520,000 ongoing to the California Privacy Protection Agency (CalPrivacy). CalPrivacy estimates that the enforcement division will require one attorney position and one information technology specialist position to investigate and enforce the prohibition on selling and sharing sensitive personal information. Although CalPrivacy currently investigates the data sharing practices of businesses, this prohibition will likely lead to a larger universe of potential targets and an increased need for analysis about data flows. (General Fund)

2) Costs to the Department of Justice (DOJ), which shares enforcement authority with CalPrivacy, potentially of a similar amount. Actual costs will depend on the extent to which the Public Rights Division pursues enforcement actions. If DOJ hires staff to handle enforcement actions, DOJ would incur significant workload costs, likely in the low hundreds of thousands of dollars annually. If DOJ does not pursue enforcement as authorized by this bill, it would likely not incur any costs.

3) Cost pressure of an unknown but potentially significant amount to the courts to adjudicate any additional filings. While the courts are not funded on a workload basis, an increase in workload could result in delayed court services and would put pressure on the General Fund to fund additional staff and resources. The FY 2026-27 Budget appropriated $70 million General Fund for this purpose. (Trial Court Trust Fund, General Fund)

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 9-5-1
YES: Bauer-Kahan, Aguiar-Curry, Bryan, Lowenthal, McKinnor, Ortega, Ward, Wicks, Wilson
NO: Macedo, DeMaio, Hoover, Irwin, Patterson
ABS, ABST OR NV: Petrie-Norris

ASM APPROPRIATIONS: 11-4-0
YES: Wicks, Aguiar-Curry, Calderon, Caloza, Fong, Mark González, Krell, Pacheco, Pellerin, Sharp-Collins, Solache
NO: Hoover, Dixon, Ta, Tangipa

ASSEMBLY FLOOR: 42-19-19
YES: Addis, Aguiar-Curry, Ahrens, Alvarez, Arambula, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Connolly, Elhawary, Fong, Gabriel, Garcia, Mark González, Haney, Hart, Jackson, Kalra, Lee, Lowenthal, Muratsuchi, Ortega, Patel, Pellerin, Quirk-Silva, Ransom, Rogers, Schiavo, Schultz, Sharp-Collins, Soria, Stefani, Ward, Wicks, Zbur, Rivas
NO: Ávila Farías, Castillo, Chen, Davies, DeMaio, Dixon, Ellis, Flora, Gallagher, Jeff Gonzalez, Hadwick, Hoover, Johnson, Lackey, Macedo, Patterson, Sanchez, Ta, Tangipa
ABS, ABST OR NV: Alanis, Carrillo, Gipson, Harabedian, Irwin, Krell, McKinnor, Nguyen, Pacheco, Papan, Petrie-Norris, Ramos, Celeste Rodriguez, Michelle Rodriguez, Blanca Rubio, Solache, Valencia, Wallis, Wilson

SENATE FLOOR: 31-4-5
YES: Allen, Alvarado-Gil, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Cortese, Durazo, Gonzalez, Grayson, Hurtado, Laird, Limón, McGuire, McNerney, Menjivar, Padilla, Pérez, Reyes, Richardson, Rubio, Smallwood-Cuevas, Stern, Umberg, Wahab, Weber Pierson, Wiener
NO: Niello, Ochoa Bogh, Seyarto, Valladares
ABS, ABST OR NV: Choi, Dahle, Grove, Jones, Strickland

UPDATED

VERSION: August 21, 2026

CONSULTANT: Julie Salley / P. & C.P. / (916) 319-2200 FN: 0004451