ASSEMBLY THIRD READING
AB 1542 (Ward)
As Introduced January 5, 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.

Major Provisions
States that a business, service provider, or contractor shall not sell or share sensitive personal information to a third party.

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 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 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
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.

FISCAL COMMENTS

1) Enforcement costs 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 (General Fund).
   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 technological analysis about data flows. The total fiscal impact for the two permanent positions is $536,000 in the first year and $520,000 ongoing.

2) Possible costs (General Fund, special funds) to the Department of Justice (DOJ), which shares enforcement authority with CalPrivacy, of an unknown amount. Actual costs will depend on whether the Attorney General pursues enforcement actions, and, if so, the level of additional staffing needed by DOJ to handle the related workload. If DOJ hires staff to handle enforcement actions authorized by this bill, DOJ would incur significant workload costs, likely in the low hundreds of thousands of dollars annually at a minimum. If DOJ does not pursue enforcement as authorized by this bill, it would likely not incur any costs.

3) Cost pressures (Trial Court Trust Fund, General Fund) of an unknown but potentially significant amount to the courts to adjudicate any additional filings. Actual costs will depend on the number of cases filed and the amount of court time needed to resolve each case. It generally costs approximately $1,000 to operate a courtroom for one hour. Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The state budget provides annual General Fund backfills to the Trial Court Trust Fund to offset revenue reductions, totaling approximately $117.3 million in 2025-26.

4) The Legislative Analyst's Office recently warned of General Fund structural deficits of around $35 billion per year beginning in the 2027-28 fiscal year.

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

UPDATED

VERSION: January 5, 2026

CONSULTANT: Julie Salley / P. & C.P. / (916) 319-2200 FN: 0002942