
THIRD READING

Bill No: AB 1542
Author: Ward (D)
Amended: 8/21/26 in Senate
Vote: 21

SENATE PRIV., DIGITAL TECH. & CONS. PROT. COMMITTEE: 7-2, 6/22/26
AYES: Cabaldon, Gonzalez, McNerney, Padilla, Reyes, Umberg, Wiener
NOES: Jones, Ochoa Bogh

SENATE APPROPRIATIONS COMMITTEE: 5-2, 8/13/26
AYES: Cervantes, Cabaldon, Grayson, Richardson, Wahab
NOES: Seyarto, Dahle

ASSEMBLY FLOOR: 42-19, 5/27/26 - See last page for vote

SUBJECT: Sensitive personal information

SOURCE: Consumer Reports
California Initiative for Technology & Democracy

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

Senate Floor amendments of 8/21/26 allow commercial credit reporting agencies to sell a consumer's social security number, as provided.

ANALYSIS:

Existing law:

1) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including 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. (Civil (Civ.) Code § 1798.100 et seq.)

2) 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 (Civ. Code § 1798.120.)

3) 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. (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).)

4) 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).)

5) 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.)

6) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (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).) 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).)

7) 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 to cooperate with law enforcement. (Civ. Code § 1798.145(a).)

8) Provides that a business does not sell or share personal information when a consumer uses or directs the business to intentionally disclose personal information or interact with one or more third parties. (Civ. Code § 1798.140.)

This bill prohibits a business, service provider, or contractor from selling or sharing the sensitive personal information of a consumer to a third party, except that a commercial credit reporting agency may sell a consumer's social security number to the extent the agency uses that information solely to identify the relationship of a consumer to a business that the consumer owns.

Background

The CCPA grants consumers certain rights with regard to their personal information, including the right to restrict the sale of information. It places attendant obligations on businesses to respect those rights. The CPRA 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, subject to relevant provisions of the CCPA, except as provided.

This bill is sponsored by Consumer Reports and the California Initiative for Technology & Democracy (CITED). This bill is supported by many privacy, consumer, labor, and other advocacy organizations, including Equality California and the California Federation of Labor Unions. This bill is opposed by industry associations, including the Association of National Advertisers and ATA Action. For a more thorough analysis, please see the Senate Privacy, Digital Technologies, and Consumer Protection Committee analysis of this bill.

Comments

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.[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 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]

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

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

---

[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 August 11, 2026.

[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/**.

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.

FISCAL EFFECT: Appropriation: No Fiscal Com.:Yes Local:No

According to the Senate Appropriations Committee:

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)

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.

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)

SUPPORT: (Verified 8/23/26)

California Initiative for Technology & Democracy, a Project of California Common CAUSE (Source)
Consumer Reports (Source)
AAPIS for Civic Empowerment
ABINE, INC. Dba Deleteme
Alliance of Californians for Community Empowerment

Asian Americans Advancing Justice Southern California
California Coalition for Worker Power
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
Center for AI and Digital Policy
CFT – a Union of Educators & Classified Professionals, AFT, AFL-CIO
Chinese Progressive Association
Coalition for Humane Immigrant Rights
Consumer Attorneys of California
Courage California
Electronic Frontier Foundation
Electronic Privacy Information Center
End Child Poverty CA
Equal Rights Advocates
Equality California
Greenlining Institute
Greenlining Institute; the
Indivisible CA Statestrong
Jewish California
LGBT Tech
Nextgen California
Oakland Privacy
Para Los Ninos
Parent Voices California
Pilipino Workers Center
Privacy Defense Alliance
Privacy Rights Clearinghouse
PWC
Reproductive Freedom for All
Secure Justice
SEIU California
Southeast Asia Resource Action Center
Tech Oversight California
TechEquity Action

Ultraviolet Action
Warehouse Worker Resource Center
Western Center on Law & Poverty
Women's Foundation California

OPPOSITION: (Verified 8/23/26)

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
Computer & Communications Industry Association
Inmarket Media, LLC
Insights Association
Internet.works
Netchoice
Network Advertising Initiative
Software Information Industry Association
Technet

ARGUMENTS IN SUPPORT: A coalition of organizations, including Techequity Action, writes:

> 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.

ARGUMENTS IN OPPOSITION: A coalition of industry associations, including the California Chamber of Commerce, writes:

While AB 1542 would continue to permit certain disclosure of sensitive PI to service providers and contractors for permitted business purposes, when it comes to all other persons and entities – “third parties,” – the bill would change the law from a “right to limit” model to a categorical prohibition. Again, under the CCPA, a third party is any “person” who is not the business with whom the consumer intentionally interacts and that collects PI (including SPI) from the consumer as a result of that current interaction with the business; a service provider to the business, or a contractor. In turn, a “person” is any individual, company, organization, or “group of persons acting in concert”. Thus, in practice, AB 1542’s ban on selling or sharing sensitive PI with third parties would significantly alter, if not constrain, several common and lawful business operations and even beneficial uses by other third parties—from business to nonprofits, to researchers, to political organizations, and government entities.

ASSEMBLY FLOOR: 42-19, 5/27/26
AYES: 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
NOES: Ávila Farías, Castillo, Chen, Davies, DeMaio, Dixon, Ellis, Flora, Gallagher, Jeff Gonzalez, Hadwick, Hoover, Johnson, Lackey, Macedo, Patterson, Sanchez, Ta, Tangipa
NO VOTE RECORDED: Alanis, Carrillo, Gipson, Harabedian, Irwin, Krell, McKinnor, Nguyen, Pacheco, Papan, Petrie-Norris, Ramos, Celeste Rodriguez, Michelle Rodriguez, Blanca Rubio, Solache, Valencia, Wallis, Wilson

Prepared by: Christian Kurpiewski / P., D.T., & C.P. / (916) 651-1548
8/24/26 11:58:24

****** END ******