SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

AB 322 (Ward)
Version: June 23, 2025
Hearing Date: July 15, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Precise geolocation information

DIGEST

This bill amends the California Consumer Privacy Act of 2018 (CCPA) to provide enhanced protections for consumers' precise geolocation information.

EXECUTIVE SUMMARY

The CCPA grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; and the right to restrict the sale of information. (Civ. Code § 1798.100 et seq.) It places attendant obligations on businesses to respect those rights. The California Privacy Rights Act of 2020 (CPRA) amended the CCPA, limited further amendment, and 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 of that information. This includes precise geolocation information.

Precise geolocation information can expose intimate details of individuals' lives, revealing where they live, work, worship, seek medical care, and spend their personal time. This information can uncover sensitive details about political affiliations, religious beliefs, health conditions, and personal relationships. Unlike other forms of data, location information is continuously generated and can be tracked in real-time, creating comprehensive surveillance profiles. This bill seeks to address the increased collection, use, and selling of consumers' precise geolocation information by requiring transparency and placing guardrails on its collection and use. The bill prohibits businesses from selling this intimate information. This bill is sponsored by Consumer Reports and the California Initiative for Technology and Democracy. It is supported by a variety of groups, including Equality California and the California Federation of Labor Unions. The bill is opposed by industry associations, including the Network Advertising Initiative and TechCA.

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 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) Establishes the CPRA, which amends the CCPA. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

3) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

4) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the following:
    a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;
    b) if the business collects sensitive personal information, 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. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and
    c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose. (Civ. Code § 1798.100(a).)

5) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting, selling, or sharing personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

6) Provides consumers the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer specified information, including the categories of personal information collected, shared, sold, and disclosed and the categories of third parties receiving the information. (Civ. Code § 1798.115.)

7) 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 this right to opt out. (Civ. Code § 1798.120.)

8) 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 biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

9) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as a consumer's "precise geolocation," which means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations. (Civ. Code § 1798.140(ae), (w).)

10) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

11) 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).)

This bill:

1) Requires a business that collects precise geolocation information to prominently display, when precise geolocation information is being collected, a notice to the consumer whose precise geolocation information is being collected that states all of the following:
    a) The fact that the consumer's precise geolocation information is being collected.
    b) The name of the business collecting the consumer's precise geolocation information.
    c) A telephone number and a website through which the consumer can obtain more information.
    d) The type of precise geolocation information collected, including the precision of the information.
    e) The goods or services requested by the consumer for which the business is collecting, processing, or disclosing the precise geolocation information and a description of how the business will process the precise geolocation information to carry out those purposes.
    f) Any disclosures of the precise geolocation information necessary to provide the goods or services requested by the consumer and the identities of the third parties to whom the precise geolocation information could be disclosed.

2) Prohibits a business that collects precise geolocation data from collecting or processing precise geolocation information more than necessary to provide the goods or services requested by the consumer. However, a business may collect or process such information if necessary to respond to security incidents, fraud, harassment, malicious or deceptive activities, or any illegal activity, as specified, or to investigate, report, or prosecute those responsible for any of those actions. Such information may not be retained for longer than 30 days.

3) Prohibits a business that collects precise geolocation data from the following:
    a) Retaining it longer than necessary to provide the goods or services requested by the consumer or longer than one year after the consumer's last intentional interaction with the business, whichever is earlier.
    b) Selling, trading, or leasing the information to a third party.
    c) Disclosing the information to a state or local government agency or official unless the agency or official serves the business or service provider of the business with a valid court order issued by a California court or a court

order from another jurisdiction that is consistent with California's laws, including the Reproductive Privacy Act and a foreign penal civil action, as defined.

d) Disclosing the information to a federal government agency unless required to do so by federal law.

4) Finds and declares that it furthers the purposes and intent of the CPRA.

COMMENTS

1. Tracking your every move

The collection, use, and monetization of precise geolocation data presents significant privacy and safety risks that many consumers may not fully appreciate and which current law may be inadequate to regulate. Precise geolocation data can reveal deeply personal and constitutionally protected behaviors: attending a protest, seeking abortion care or legal services, visiting a place of worship, visiting an LGBTQ community center, or organizing a union. Today, this data is quietly collected by apps and devices, traded by data brokers, and accessed by government agencies—often without a court order or consumer knowledge:

> For many of us, our mobile phone is a constant companion, with us wherever we go. It's also constantly collecting information about us, what we do, and where we do it. And unbeknownst to many of us, once that information is collected, much of it gets sold onwards in a murky marketplace of data brokers and advertisers. Because this market for our data is not transparent, it's almost impossible to figure out who has information about us and what they're doing with it.
>
> Our phones can also reveal far more about us than we might realize: important details about our lives and where we've been. For example, our phones might be periodically sending their exact location to tech companies. This data can pinpoint our comings and goings with startling precision. Think what this might reveal: what therapist you're seeing, what medical treatment you're seeking, your visits to places of worship, and even your reproductive choices. This type of tracking can cause enormous harm to consumers, including stigma, emotional distress, discrimination, or even physical violence.[1]

[1] Carol Kando-Pineda. *Consumer Alert: FTC sues company that sells consumers' sensitive location information* (August 29, 2022) FTC, https://consumer.ftc.gov/consumer-alerts/2022/08/ftc-sues-company-sells-consumers-sensitive-location-information. All internet citations are current as of June 27, 2025.

The scope of the problem is evident from the number of enforcement actions the Federal Trade Commission has taken in recent years:

> The Federal Trade Commission is taking action against Gravy Analytics Inc. and its subsidiary Venntel Inc. for unlawfully tracking and selling sensitive location data from users, including selling data about consumers' visits to health-related locations and places of worship.
>
> Under a proposed order settling the FTC's allegations, Gravy Analytics and Venntel will be prohibited from selling, disclosing, or using sensitive location data in any product or service, and must establish a sensitive data location program.
>
> The FTC's complaint alleges that Gravy Analytics and Venntel violated the FTC Act by unfairly selling sensitive consumer location data, and by collecting and using consumers' location data without obtaining verifiable user consent for commercial and government uses.
>
> According to the complaint, Gravy Analytics continued to use consumers' location data after learning that consumers didn't provide informed consent. Gravy Analytics also unfairly sold sensitive characteristics, like health or medical decisions, political activities and religious viewpoints, derived from consumers' location data.
>
> "Surreptitious surveillance by data brokers undermines our civil liberties and puts servicemembers, union workers, religious minorities, and others at risk," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "This is the FTC's fourth action taken this year challenging the sale of sensitive location data, and it's past time for the industry to get serious about protecting Americans' privacy."[2]

2. Getting serious about privacy

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.

---

[2] Press Release, *FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites* (December 3, 2024) FTC, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers.

The CCPA provides adult consumers the right, at any time, to direct a business not to sell or share personal information about the consumer to third parties. 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.

The CPRA added a new category of information, sensitive information, which includes precise geolocation information, which is defined as any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet. Consumers are empowered to limit businesses' use of such information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer. However, concerns have been raised that these protections are not enough given the sensitivity of this data and its widespread and systematic collection.

This bill responds to the growing problem by amending the CCPA to require more transparency around when, how, and for what purposes businesses are collecting and using precise geolocation information and placing clear restrictions on what they can do with it.

First, the bill requires that businesses prominently display a notice when precise geolocation information is being collected from a consumer. This must include information about the business collecting it, the basis for the collection, and any disclosures of it necessary to provide the consumer the goods and services requested.

Next, the bill places a number of restrictions on what businesses can do with this information. Businesses are limited to collecting and processing only the precise geolocation information necessary to provide the goods or services requested by the consumer, except as specified, including for responding to security incidents and fraud. Businesses must not retain this information for longer than necessary to provide those goods and services.

To directly address the opaque market for this information, the bill enacts a prohibition on the selling, trading, or leasing of precise geolocation information to a third party. California joins other states, including Oregon and Maryland in so banning sales of this information.[3]

Given the sensitive nature of this information and the increasing hostility from the federal government and other states toward certain communities in California, limitations on sharing with government agencies is also included in the bill. The bill prohibits businesses from disclosing precise geolocation information to a state or local

[3] Suzanne Smalley, *Oregon becomes second state to ban sale of precise geolocation data* (May 28, 2025) The Record, https://therecord.media/oregon-passes-geolocation-kids-data-bill.

government agency or official unless the agency or official serves the business or service provider of the business with a valid court order issued by a California court or a court order from another jurisdiction that is consistent with California's laws, specifically including the Reproductive Privacy Act. They are also prevented from disclosing precise geolocation information to a federal government agency unless required to do so by federal law.

Demonstrating the need for this, it has widely been reported that federal agencies, including the United States Immigration and Customs Enforcement (ICE), have contracted with data brokers for their troves of personal information and specifically to get around jurisdictions' sanctuary laws and "allowing agencies like [ICE] to circumvent traditional avenues of information gathering for which it typically would have to show probable cause."[4] Such information in the hands of local law enforcement has also raised concerns as multiple California sheriffs have expressed their intention to cooperate with ICE, with one vowing "to work 'around' California law to assist federal immigration enforcement."[5] Recent events here in California underscore the urgent need for such protections. In a recent piece in the Sacramento Bee, entitled "Recent ICE raids expose just how vulnerable our location data is," the role of location data in the terrorizing of our communities is revealed:

> The frightening images of recent Immigration and Customs Enforcement (ICE) raids have sown fear and uncertainty throughout California. As horrifying as these military-type operations are, what's just as chilling is how it's happening: the quiet, invisible role of location data in making these raids possible. Through commercial data brokers and partnerships with local law enforcement, ICE has amassed a vast and powerful collection of data that allows them to track individuals' movements with unnerving precision. This might sound like science fiction, but it's our present reality. Location surveillance is omnipresent — whether through automated license plate readers, mobile device tracking or facial recognition in public spaces. The same data we generate by simply carrying a phone or driving down the street can now be weaponized against any one of us.

---

[4] Johana Bhuiyan, *US immigration agency explores data loophole to obtain information on deportation targets* (April 20, 2022) The Guardian, https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets.

[5] Nigel Duara, *A California sheriff is planning to break the state's sanctuary law. Here's how* (February 28, 2025) CalMatters, https://calmatters.org/justice/2025/02/sanctuary-state-amador-sheriff/; *see also* Guardian staff, *San Diego sheriff says she won't honor county's 'sanctuary' immigration policy* (December 11, 2024) The Guardian, https://www.theguardian.com/us-news/2024/dec/11/san-diego-sanctuary-immigration-deportation-policy#:~:text=San%20Diego%20sheriff%20says%20she,policy%20%7C%20San%20Diego%20%7C%20The%20Guardian.

> The evidence is right in front of us: In 2019, the American Civil Liberties Union revealed that ICE had been using driver location data from local police to facilitate deportations. More recently, reporting shows how ICE and the Department of Homeland Security are expanding these tools through deals with the Internal Revenue Service and private data brokers.[6]

According to the author:

> With the rapid growth of the location data 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 No Californian should have their daily movements tracked, sold, or exploited just for going about their lives. Whether you're commuting to work, visiting a doctor, or dropping your kids off at school, your location data should remain private. AB 322 draws a clear line—it puts the safety and privacy of everyday Californians first.

3. Stakeholder positions

Consumer Reports, a sponsor of the bill, emphasizes the need for the bill:

> The location information market is a multi-billion-dollar industry centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices and often without their knowledge or explicit consent. Location data is an extremely sensitive form of personal information. Researchers have shown that 95 percent of individuals can be uniquely identified from just four location points in time and 50 percent of individuals can be uniquely identified from just two spatio-temporal points; most companies that collect this information have orders of magnitude more data than that.
>
> Much of this information is amassed by data brokers, entities that compile extensive dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior, as well as inferences about individuals based on their information. Some companies collect and share consumers' location information as often as every three seconds. This information is then sold

[6] David Trujillo & Jonathan Mehta Stein, *Recent ICE raids expose just how vulnerable our location data is* (June 26, 2025) The Sacramento Bee, https://www.sacbee.com/opinion/op-ed/article309312170.html.

> and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process. This activity poses a host of significant risks to California residents.

Writing in support, the Alliance for TransYouth Rights states:

> As smartphones and connected devices become ever-present in our daily lives, so does the potential for intrusive surveillance. The ability to monitor individuals' movements with pinpoint accuracy presents risks to personal safety and civil liberties, especially for communities that have historically faced disproportionate levels of surveillance, including immigrants, LGBTQ+ individuals, and people seeking reproductive healthcare.
>
> AB 322 takes a bold and necessary stand for privacy in the 21st century. By banning the sale or lease of precise geolocation data and requiring government agencies to obtain a warrant for access, this bill restores vital safeguards to Californians' digital lives. It reflects and reinforces California's leadership in technology, civil rights, and consumer protection.

A coalition of industry groups, including TechNet, writes in opposition:

> It would be incredibly (and unreasonably) difficult if not impossible to constantly signal to a consumer that location data is being collected when that is necessary for the services. When a business seeks to collect precise geolocation information from a consumer's device via an app, for example, the app itself is not the entity directly obtaining the consumer's permission. From both a technical and privacy standpoint, apps receive a device's precise geolocation information only if device users enable the sharing of that information with specific apps in the devices' settings menu. In other words, although apps can provide users with information in their apps about how precise geolocation information will be used, the actual act of collecting the information for the first time – and the presentation of notices to consumers when the permission is actually sought – happens in devices' settings menus, not in apps.
>
> As such, subdivision (a) could be read to mean that apps would be required to somehow present notices to consumers in devices' settings menus - something apps have no control over. It could also be read to mean that a notice would have to be presented to consumers for the entire duration of time during which their precise geolocation is being collected. This would not be possible to do without significantly degrading consumers' experiences.

A coalition of advocacy and labor groups, including the California Partnership to End Domestic Violence and the California Federation of Labor Unions, writes in strong support:

> Location data is among our most sensitive information. When collected across time, this information can reveal every aspect of a person's life, such as medical conditions, sexual orientation, political activities, and religious beliefs. This type of data has been used by scammers to facilitate financial fraud, retailers to generate differential pricing, and can be aggregated and shared with a number of other bad actors. Additionally, it is imperative we protect the privacy rights of our communities, especially with increased attacks targeting immigrants, Black and Brown community members, LGBTQ people, and individuals seeking reproductive health care. California must take bold action to ensure consumers are protected and their location information is secure. AB 322 answers this call.

SUPPORT

California Initiative for Technology and Democracy (sponsor)
Consumer Reports (sponsor)
AAPIs for Civic Empowerment
Alliance for TransYouth Rights
Asian Americans Advancing Justice Southern California
California Civil Liberties Advocacy
California Federation of Labor Unions, AFL-CIO
California Nurses Association
Center for Democracy and Technology
Center for Digital Democracy
Consumer Federation of America
Courage California
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Equality California
Kapor Center
LGBT Tech
PFLAG Sacramento
Secure Justice
TechEquity Action
Ultraviolet Action
Viet Rainbow of Orange County

OPPOSITION

Association of National Advertisers

California Baptist for Biblical Values
California Chamber of Commerce
California Retailers Association
Computer and Communications Industry Association
CTIA
Network Advertising Initiative
Security Industry Association
Software Information Industry Association
State Privacy and Security Coalition, Inc.
TechCA
TechNet

RELATED LEGISLATION

Pending Legislation:

SB 44 (Umberg, 2025) amends the CCPA to require a "covered business" to use neural data collected through a brain-computer interface only for the purpose for which it was collected. It requires the covered business to delete the data when the purpose for which it is collected is accomplished. SB 44 is currently in the Senate Appropriations Committee.

SB 361 (Becker, 2025) fortifies the Data Broker Registry law by requiring additional disclosures from data brokers on the types of information collected. SB 361 is currently in the Assembly Appropriations Committee.

AB 894 (Carrillo, 2025) requires a general acute care hospital to inform a patient that the patient may restrict or prohibit the use or disclosure of protected health information in the hospital's patient directory, as provided for in federal regulations, as specified. AB 894 is currently in the Senate Appropriations Committee.

AB 1337 (Ward, 2025) amends the Information Practices Act (IPA) by expanding the definition of "personal information," extending its scope to cover local governmental entities, and bolstering protections regarding disclosures and accounting. AB 1337 is currently in this Committee and is being heard the same day as this bill.

Prior Legislation: AB 947 (Gabriel, Ch. 551, Stats. 2023) added citizenship and immigration status to the definition of "sensitive personal information" in the CCPA, affording it greater protections.

PRIOR VOTES:

Prior votes irrelevant to current version of this bill

****