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

AB 566 (Lowenthal)
Version: June 2, 2025
Hearing Date: July 1, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Consumer Privacy Act of 2018: opt-out preference signal

DIGEST

This bill requires browsers and browser engines to include a setting that enables a consumer to send an opt-out preference signal to a business with which a consumer interacts through the browser.

EXECUTIVE SUMMARY

The California Consumer Privacy Act (CCPA) grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; and protection from discrimination for exercising these rights. (Civ. Code § 1798.100 et seq.) In the November 3, 2020 election, voters approved Proposition 24, which established the California Privacy Rights Act of 2020 (CPRA). The CPRA amends the CCPA, limits further amendment, and creates the California Privacy Protection Agency (PPA). Relevant here, the CCPA 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 of their opt-out right.

This bill seeks to empower consumers to exercise this right more meaningfully in the many interactions they have with businesses online. It prohibits a business from developing or maintaining a browser or browser engine that does not include a setting that enables a consumer to send an opt-out preference signal to a business with which the consumer interacts through the browser. The setting must be easy for a reasonable person to locate and configure. This bill is sponsored by the California Privacy Protection Agency. It is supported by a number of privacy and consumer advocacy groups as well as technology companies, including Mozilla and the Center for Digital Democracy and Consumer Reports. No timely opposition was received.

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) 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 that selling and sharing. (Civ. Code § 1798.120.)

3) Prohibits a business, notwithstanding the above, from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. (Civ. Code § 1798.120(c).)

4) Provides a business shall not be required to comply with the requirement to place a clear and conspicuous link to opt out if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations. (Civ. Code § 1798.135.)

5) 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. (Civ. Code § 1798.140(ae).)

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

7) 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) Establishes the California Opt Me Out Act.

2) Prohibits a business from developing or maintaining a browser or browser engine that does not include a setting that enables a consumer to send an opt-out preference signal to a business with which the consumer interacts through the browser. This required setting must be easy for a reasonable person to locate and configure.

3) Requires a business that develops or maintains a browser or browser engine to make clear to a consumer in its public disclosures how the opt-out preference signal works and the types of personal information to which the signal would apply.

4) Authorizes the PPA to adopt regulations as necessary to implement and administer this law.

5) Defines the relevant terms:
   a) "Browser" means an interactive software application that is used by consumers to locate, access, and navigate internet websites.
   b) "Browser engine" means the software component of a web browser or web-enabled application that interprets and renders web content, including HTML, CSS, and JavaScript, transforming code into interactive visual output on a consumer's device, including, but not limited to, Blink, Gecko, and WebKit.
   c) "Opt-out preference signal" means a signal that complies with this title and that communicates the consumer's choice to opt out of the sale and sharing of the consumer's personal information.

6) Includes findings and declarations that this law furthers the purposes and intent of the CPRA.

<u>COMMENTS</u>

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.

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 or shares personal information to third parties is required to notify consumers that this information may be sold or shared and that they have the right to opt out of such sales. (Civ. Code § 1798.120(b).)

2. Providing tools to effectuate consumer rights

Despite this right to opt out, many consumers are simply overwhelmed with meaningfully exercising this right given all the businesses that the consumer interacts with online. According to research by Consumer Reports:

> The CCPA's opt-out model is inherently flawed; it places substantial responsibility on consumers to identify the companies that collect and sell their information, and to submit requests to access it, delete it, or stop its sale. Even when companies are making a good-faith effort to comply, the process can quickly become unmanageable for consumers who want to opt out of data sale by hundreds if not thousands of different companies.[1]

The report found that consumers struggled to locate the required links and were forced to navigate through confusing disclosures. The report offered up a number of policy recommendations, including that consumers should have access to browser privacy signals that allow them to opt out of all data sales in one step.

[1] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* (October 1, 2020) Consumer Reports, https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf [as of June 21, 2025].

Previous attempts have been made to achieve this sort of mechanism, including when nearly all major browser vendors adopted "Do Not Track," a technology that allowed consumers to transmit "Do Not Track" requests to businesses via their web browser. However, there was no legal requirement to honor these signals.

More recently Global Privacy Control entered the market. It is a browser setting that notifies websites of a consumer's privacy preferences, such as not sharing or selling their personal information, with each website the consumer visits.

The CCPA requires businesses to honor opt-out preference signals as a request to opt-out of sale of their personal information. The California Department of Justice (DOJ) included this in their CCPA regulations, adopted in 2020. The PPA's regulations, adopted in 2023, updated the opt-out preference signal requirement.

The author argues that now that California businesses receiving opt-out preference signals are required to honor them under the CCPA, there is a significant opportunity to expand consumer access by requiring browsers to offer similar preference signals to consumers. This bill provides that a business shall not develop or maintain a browser or browser engine that does not include a setting that enables a consumer to send an opt-out preference signal to a business with which the consumer interacts through the browser. It requires the setting to be easy for a reasonable person to locate and configure. The bill authorizes the PPA to adopt regulations.

According to the author:

> Californians have the right to easily opt-out of the sale of their personal information through opt-out preference signals, yet a significant number of leading web browsers do not offer such signals. Consumers are often unaware of how their data is being collected and shared when they are using the internet, which leads to the misuse of their personal data.
>
> AB 566 makes it easier for consumers to state their privacy preferences from the start by requiring web browsers to allow a user to exercise their opt-out rights at all businesses with which they interact online in a single step.

It should be noted that a substantially similar bill was passed by the Legislature last year, AB 3048 (Lowenthal, 2024). AB 3048 was vetoed by Governor Newsom, who stated in his message:

> This bill would require internet browsers and mobile operating systems to include a setting that California consumers can use to signal to businesses with which they interact that they wish to, first, opt out of the sale or

> sharing of their personal information, and second, limit use of their sensitive personal information.
>
> I share the author's desire to enhance consumer privacy. Last year, I signed SB 362 (Becker), which requires the California Privacy Protection Agency to establish an accessible deletion mechanism allowing consumers to request that data brokers delete all of their personal information.
>
> I am concerned, however, about placing a mandate on operating system (OS) developers at this time. No major mobile OS incorporates an option for an opt-out signal. By contrast, most internet browsers either include such an option or, if users choose, they can download a plug-in with the same functionality. To ensure the ongoing usability of mobile devices, it's best if design questions are first addressed by developers, rather than by regulators.

In response to this veto message, this bill does not place obligations on operating systems, but rather limits its focus to browsers and browser engines.

Relevant here, and cited by the Governor above, SB 362 (Becker, Ch. 709, Stats. 2023) established the Delete Act, which bolstered the data broker registry law by, in part, requiring more information to be reported and transferring much of the relevant duties from DOJ to the PPA. More importantly, it also expanded consumers' deletion rights and requires the PPA to create an accessible deletion mechanism that allows a consumer, through a single request, to request that every data broker delete the personal information related to the consumer and held by the data broker, except as specified. To ensure consumers can meaningfully exercise their rights under the law given the hundreds of data brokers on the registry, the mechanism is required to support the ability of a consumer's authorized agent to aid in the deletion request.

3. <u>Stakeholder positions</u>

This bill is sponsored by the PPA, which explains the need for the bill:

> Opt-out preference signals like the Global Privacy Control (GPC) are important innovations as they significantly simplify consumers' ability to exercise their rights at scale to opt-out of sale under the California Consumer Privacy Act (CCPA) by enabling them, in a single step, to send an opt-out request to every site they interact with online. The CCPA currently requires businesses to honor opt-out preference signals as a request to opt-out of the sale of their personal information. The California Department of Justice included this in their CCPA regulations, adopted in 2020 and the CPPA's regulations, adopted in 2023, update the opt-out preference signal requirement.

> However, only a handful of browsers currently offer native support for opt-out preference signals. Importantly, none are loaded onto devices by default, making it difficult for consumers to learn about and take advantage of these protections. Google Chrome, Microsoft Edge, and Apple Safari—which make up over 90% of the desktop browser market share—have declined to offer these signals.
>
> In addition, while major browsers including Google have rebuffed calls to offer opt-out preference signals to support consumers, Google has simultaneously introduced new practices in the last few months that further erode Californians' privacy. In February of 2025, Google updated its policies to allow its ad partners to use digital fingerprinting technologies to identify users and collect information about them. Fingerprinting allows businesses to collect information about a device's hardware or software which can easily be combined with other data to uniquely identify a user. As critics, including the UK's data protection authority have pointed out, this technology largely operates unknown to the user and outside of their control. One of the best ways for a consumer to limit the privacy harms of digital fingerprinting is for consumers to be able to send opt-out preference signals.

A coalition of tech companies and advocacy groups in support, including Brave Software and the Electronic Privacy Information Center, write:

> Opt-out preference signals were a policy response to the suboptimal consumer rights formulation under the initial version of the CCPA, which required consumers to effectuate their opt-out requests individually with each business with which they interacted. That meant that consumers with a generalized preference not to allow the sharing or selling of their personal information would have had to contact hundreds, if not thousands, of businesses in order to satisfy that preference.
>
> As Consumer Reports testing showed, the individual opt-out structure was intensely cumbersome for consumers – many consumers struggled to complete an opt-out request on just a single data broker's website – an arrangement that depresses the usage of consumer rights under the law. Opt-out preference signals were intended to relieve this burden and make it easier for consumers to express their privacy preferences.
>
> Subsequent to the passage of CPRA's amendments to the CCPA that created the opt-out preference signal requirement (as well the enactment of several other state privacy laws that create similar requirements), we've seen numerous privacy-conscious browser vendors, such as Brave, DuckDuckGo, and Firefox support the concept of opt-out preference

> signals. Most commonly, such browsers do so by enabling usage of Global Privacy Control, a technical specification that has been interpreted by the California Privacy Protection Agency and California Attorney General to serve as a permissible opt-out preference signal under the CCPA. These browsers typically either enable the GPC signal to be sent by default or make it a setting the user can easily toggle on or off.
>
> However, the largest browser vendors (Apple Safari, Google Chrome, and Microsoft Edge, which cumulatively enjoy more than 90% of the browser share in the United States) currently do not provide native support for opt-out preference signals. Today, if a user wants to send an opt-out preference signal on Chrome, Safari, or Edge, they need to download a third-party extension to do so, while a mobile platform user cannot configure their device to send an opt-out preference signal at all. As a result, millions of Californians, while technically enjoying the right to send such a signal, likely have no idea that this right even exists and have no easy way of acting on it even if they did. . . .
>
> AB 566 will ensure that consumers have the ability to use their privacy rights by requiring that browser vendors and browser engines include an easy to locate and use setting that enables the consumer to send an opt-out preference signal. This bill's approach will help reduce opt-out friction and make it easier for California residents to control their data, while also providing for flexibility by allowing the CPPA to adopt rules that will allow the law to keep pace with technology.

Writing in support, Oakland Privacy explains why existing law and options are inadequate:

> California has come too far down this particular road to pursue any other avenue than robust opt-out protocols. User testing, from Consumer Reports among others, has documented that even motivated users find the current opt-out options to be repetitive, confusing and burdensome.
>
> The operators of the world's largest Internet browsers, most notably Alphabet (which runs Chrome) and Microsoft (which operates Edge), have declined to adopt an opt-out preference signal to allow users of their browser to indicate they don't want their personal information sold or shared by any URL they visit while using the browser. Chrome, in particular, has stubbornly insisted on incorporating an opt-out preference signal only as a browser extension, an add-on piece of software users have to locate and install themselves. Apple, despite its marketing as a more privacy-friendly tech giant, has also declined a straightforward installation of a preference signal, preferring to instead develop

proprietary cookie delimiters for Safari, their browser for iOs. Some smaller browsers like Firefox, Brave and Opera have, or are in the process of, implementing a browser preference signal, but they are used by much smaller segments of the general Internet user base.

4. Furthering the purpose and intent of the CPRA

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.

The bill ensures a pathway for consumers to more effectively exercise their rights under the CCPA. Therefore, as it explicitly states, this bill "furthers the purposes and intent of the California Privacy Rights Act of 2020."

SUPPORT

California Privacy Protection Agency (sponsor)
Access Humboldt
Brave Software
Center for Democracy and Technology
Center for Digital Democracy
Center for Economic Justice
Common Sense Media
Concept Art Association
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Reports

Consumer Watchdog
Digital Content Next
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Los Angeles County Democratic Party
Mothers Against Media Addiction
Mozilla
Oakland Privacy
Privacy Rights Clearinghouse
Santa Monica Democratic Club
Secure Justice
Tech Oversight California

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

SB 361 (Becker, 2025) expands the disclosures that data brokers must make when registering with California's Data Broker Registry. SB 361 is currently in the Assembly Appropriations Committee.

AB 656 (Schiavo, 2025) requires large social media platforms to provide users with a clear and accessible mechanism for deleting their accounts and associated personal information. AB 656 is currently in this Committee and is set to be heard the same day as this bill.

Prior Legislation:

AB 3048 (Lowenthal, 2024) *See* Comment 2.

SB 362 (Becker, Ch. 709, Stats. 2023) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 53, Noes 1)
Assembly Appropriations Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 9, Noes 0)
****