
CALIFORNIA PRIVACY PROTECTION AGENCY

400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov



Date: July 13, 2026

To: California Privacy Protection Agency Board
(Meeting of August 7, 2026)

From: Maureen Mahoney, Deputy Director of Policy and Legislation
California Privacy Protection Agency

Subject: **Agenda Item 12 — Legislative Update and Authorization of Agency Positions on Pending Legislation. SB 435 (Wahab, CCPA: personal information: exemptions)**

SB 435, authored by Senator Wahab, seeks to strengthen privacy rights by narrowing the category of publicly available information that is exempt from personal information protected by the California Consumer Privacy Act.¹ The bill is currently in Assembly Appropriations. Staff recommends a support position because the bill meaningfully increases privacy protections for Californians.

Summary

The California Consumer Privacy Act (CCPA) provides key consumer privacy rights to Californians. The rights granted include the right to know what personal information businesses have collected and how that information is being used, sold, and shared; the right to delete personal information; the right to correct inaccurate personal information, the right to limit a business's use and disclosure of sensitive personal information to certain business purposes, and the right to stop businesses' sale and sharing of personal information, among other protections.

Similarly, the Delete Act allows a consumer, through an accessible deletion mechanism known as the Delete Request and Opt-Out Platform (DROP), to make a single verifiable request that every data broker that maintains personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor. The Delete Act requires data brokers to access DROP at least once every 45 days and to process any deletion requests within 45 days of receipt.² The Delete Act incorporates by reference the definition of personal information from the CCPA, so changes to the CCPA definition impact the operation of the Delete Act.³

¹ SB 435 (June 9, 2026)

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB435

² Civ. Code § 1798.99.86.

³ Civ. Code § 1798.99.80(a).

The majority of the rights and obligations provided by the CCPA and the Delete Act apply to personal information, defined as information that identifies, relates to, or could reasonably be linked with a particular consumer or household.⁴ Sensitive personal information is a subset of personal information that includes, among other things, social security numbers, precise geolocation information, citizenship or immigration status, genetic data, and the contents of messages.⁵ Personal information and the subset of sensitive personal information, however, do not include publicly available information. Under existing law, publicly available information includes:

- (I) Information that is lawfully made available from federal, state, or local government records.
- (II) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or through widely distributed media.
- (III) Information made available by a person to whom the consumer disclosed the information if the consumer has not restricted the information to a specific audience.⁶

Consumer rights provided under the CCPA and the Delete Act do not apply to information that falls into these three categories. The CCPA also specifies, however, that publicly available does not include biometric data collected without the consumer's knowledge.⁷

This bill amends the CCPA to narrow the definition of "publicly available." First, the bill deletes the third category entirely. Second, the bill amends the second category as follows:

- (II) Information that ~~a business has a reasonable basis to believe~~ is lawfully made available to the general public by the consumer or from widely distributed media.⁸

Analysis

In staff's view, this bill narrows the publicly available exception to better reflect the realities of online information sharing and meaningfully expands the protections of the CCPA to data over which consumers would reasonably expect to have control. Such an expansion reduces the sensitive data that is freely available for data brokers to collect and sell, minimizing privacy harms to consumers. Indeed, the author's fact sheet for the bill focuses largely on data broker products that specifically market the sale of sensitive "publicly available" information to federal law enforcement and immigration agencies.⁹

⁴ Civ. Code § 1798.140 (v).

⁵ Civ. Code § 1798.140 (ae).

⁶ Civ. Code § 1798.140(v)(2)(A).

⁷ Civ. Code § 1798.140(v)(2)(B)(ii).

⁸ SB 435 (June 9, 2026),

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB435.

⁹ Dr. Aisha Wahab, Assistant Senate Majority Leader, Fact Sheet for SB 435: Defending Californians' Privacy Act, June 11, 2026.

First, removing the third exempted category of the definition of publicly available closes a loophole that could potentially allow shared information to be considered “publicly available” simply because a consumer does not affirmatively clarify in each online interaction that the information is restricted to certain audience. This loophole potentially allows a significant amount of personal information to fall outside of the CCPA even if a consumer would not reasonably consider the information to be publicly available. In today’s online ecosystem, individuals share personal information with companies hundreds of times a day and are rarely afforded meaningful opportunity up front to restrict further distribution. Additionally, consumers that provide information in one context for a specific service or purpose rarely expect or anticipate that it will be shared or used in another context. Removing this category brings the law in line with online information sharing realities and consumers’ expectations of privacy.

Second, removing the “reasonable basis to believe” standard from the second category of the definition of publicly available ties the exemption to consumers’ actions and intentions rather than businesses’ subjective belief. Whether a consumer has made information available to the public is a question of fact, not a matter of the business’s judgment, however the current language allows businesses to escape the obligations of the CCPA simply by asserting a belief. Such a rule gives businesses and data brokers wide berth to claim that information shared or identified online has been made public without thorough consideration of the consumer’s true intent. Personal information that has not been made public by the consumer should not be exempted from protection because a business mistakenly believes the information is public.

Taken together, these changes help address the privacy risks posed by the mass scraping of online data and unfettered information collection by data brokers. Data brokers regularly buy, sell, and scrape from the internet information that is classified as “publicly available,” using it to build detailed profiles of individuals that are available for sale to anyone, including bad actors and government agencies.¹⁰ This data can then be used to profile and harm consumers. For example, the Agency recently brought an action to stop a data broker from selling lists of people with Alzheimer’s disease, leaving them vulnerable to targeting by malicious actors.¹¹

This bill minimizes these risks by reducing what information is classified as publicly available. The modifications address the false assumption that information that is shared in a transaction or accessible in one online context is intended to be public. Rather, this bill extends or removes protections based on consumer expectations.

For these reasons, staff recommends supporting this bill.

Recommendation: Support

¹⁰ Jude Joffe-Block, *Your data is everywhere. The government is buying it without a warrant*, NPR (March 25, 2026), <https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic>.

¹¹ *CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers* (January 8, 2026), <https://privacy.ca.gov/2026/01/calprivacy-brings-new-round-of-enforcement-actions-against-data-brokers/>

Public Support/Opposition:

Per the June 20 Assembly Privacy Committee bill analysis:¹²

Support:

Alliance for a Better Community (UNREG)
Alliance for Boys and Men of Color
Alliance for Children's Rights
Asian Americans Advancing Justice Southern California
California State PTA
California Teachers Association
Children's Advocacy Institute
Consumer Reports
Consumer Watchdog
Courage California
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice
SEIU California
UnidosUS
University of California Student Association

Opposition:

Association of National Advertisers
California Chamber of Commerce
Computer & Communications Industry Association
Consumer Data Industry Association
CSPRA
Insights Association
Software Information Industry Association
State Privacy and Security Coalition
TechCA
TechNet

Staff Contact: Maureen Mahoney, Deputy Director of Policy & Legislation

maureen.mahoney@coppa.ca.gov

¹² California Assembly Privacy & Consumer Protection Committee Analysis at 15 (June 20, 2026), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202520260SB435.