SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

SB 1104 (Cabaldon)
Version: April 9, 2026
Hearing Date: April 20, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Consumer Privacy Act of 2018: data broker registration: accessible deletion mechanism

DIGEST

This bill requires data brokers to provide more information when registering with the data broker registry and codifies existing regulatory language defining what a "direct relationship" is. The bill requires the California Privacy Protection Agency (CalPrivacy) to create a "privacy preference profile tool."

EXECUTIVE SUMMARY

Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection provides consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of California's Constitution. One particularly troubling area of this systematic data collection is the emergence of data brokers that collect and profit from this data without having any direct relationship with the consumers whose information they amass.

In order to bring this industry into the light, California established a data broker registry, which requires data brokers to register annually with CalPrivacy. Data brokers are required to pay a fee and provide certain information about themselves and their practices. Recent updates have bolstered the law to provide consumers more control over their information and expanded consumers' deletion rights, including through the creation of an accessible deletion mechanism. This bill again fortifies the law by requiring additional disclosures from data brokers and refining the definition of data broker. The bill also requires CalPrivacy to create a privacy preference profile tool, providing consumers the ability to distinguish between the hundreds of data brokers. This bill is author-sponsored. No timely support or opposition has been received by the Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Requires a business, on or before January 31 following each year in which it meets the definition of a data broker, to register with CalPrivacy, as provided. (Civ. Code § 1798.99.82.)

2) Defines "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The definition specifically excludes the following:
   a) an entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
   b) an entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations; and
   c) an entity to the extent that it is covered by the Insurance Information and Privacy Protection Act, Insurance Code § 1791 et seq. (Civ. Code § 1798.99.80.)

3) Requires data brokers to provide, and CalPrivacy to include on its website, the name of the data broker and its primary physical, email, and website addresses, as well as various other disclosures, including whether the broker collects consumers' precise geolocation or reproductive health care data and whether they collect the personal information of minors. Data brokers may, at their discretion, also provide additional information concerning their data collection practices. (Civ. Code §§ 1798.99.82, 1798.99.84.)

4) Subjects a data broker that fails to register as required to administrative fines and costs to be recovered in an administrative action brought by the PPA. (Civ. Code § 1798.99.82.)

5) Requires the PPA to establish an accessible deletion mechanism, as provided, that allows consumers, through a single request, to request all data brokers to delete any personal information related to the consumer, as specified. Data brokers are required to regularly access the mechanism and process requests for deletion, as specified. (Civ. Code § 1798.99.86.)

6) Provides that after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant hereto, the data broker must delete all personal information of the consumer, except as provided, beginning August 1, 2026. After a consumer has submitted a deletion request and a data broker has deleted the consumer's data, the data broker shall not sell or share new personal information of the consumer unless the consumer requests otherwise or the selling or sharing of the information is otherwise permitted, as

provided. Requires data brokers to undergo audits every three years to determine compliance with the data broker registry law. (Civ. Code § 1798.99.86.)

7) 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.)

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

9) 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.)

10) 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) Defines, for purposes of the definition of a data broker, "direct relationship" as meaning that a consumer has intentionally interacted with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services. A "direct relationship" requires a consumer to intend to interact with the business.

2) Provides that a business does not have a "direct relationship" with a consumer because it collects personal information directly from the consumer. A business also does not have a "direct relationship" with a consumer as to personal information it sells about the consumer that it collected outside of a first-party

interaction with the consumer. "First party" means a consumer-facing business with which the consumer intends and expects to interact.

3) Requires data brokers to disclose whether they sell inferences about the attributes of a consumer based on their analysis of the personal information of minors or the consumer's citizenship data, union membership, sexual orientation, gender identity, gender expression, or reproductive health care data.

4) Requires CalPrivacy to create a privacy preference profile tool that enables a consumer to:
    a) Define and store a privacy preference profile expressing the consumer's preferences regarding data broker data collection and use practices.
    b) Use the profile to identify registered data brokers whose disclosed practices are consistent with the consumer's preferences so that a consumer may make an informed decision as to whether to exclude those data brokers from a deletion request.

5) Requires CalPrivacy, in designing the above tool, to consider input modalities that optimize comprehensibility and alignment with consumer intent and minimize cognitive load, including a natural language input or a structured schematic interface.

6) Requires the tool to evaluate each registered data broker's most recent annual registration disclosures against the consumer's preference profile and shall categorize each data broker as one of the following:
    a) "Consistent," if the data broker's disclosed practices are compatible with the consumer's stated preferences across all profile dimensions the consumer has specified.
    b) "Inconsistent," if the data broker's disclosed practices conflict with the consumer's stated preferences on one or more dimensions.
    c) "Indeterminate," if the data broker's registration is silent, ambiguous, or incomplete with respect to a profile dimension that is material to the consumer's preferences. The tool shall display the specific gap in disclosure that produced this categorization. In the absence of a consumer instruction to the contrary, a data broker categorized as indeterminate shall be treated as inconsistent for purposes of the accessible deletion mechanism exclusion. The tool shall permit the consumer to override this default for individual data brokers.

7) Requires the tool to display the list of registered data brokers categorized pursuant to the above prior to the consumer's submission of a deletion request through the accessible deletion mechanism.

8) Provides that the consumer may, with explicit confirmation for each data broker or for all data brokers categorized as consistent collectively, elect to exclude any data broker categorized as consistent from a pending deletion request.

9) Requires the tool to clearly inform the consumer, prior to any exclusion, of all of the following:
    a) That exclusion means the data broker will not be directed to delete the consumer's personal information.
    b) That the categorization is based solely on the data broker's self-reported registration disclosures and not on independently verified practices.
    c) That the consumer may at any time resubmit a request that includes previously excluded data brokers.

10) Provides that exclusion of a data broker from a deletion request does not constitute consent by the consumer to the data broker's data practices and does not limit any right the consumer may exercise under the CCPA or any other state law.

11) Requires CalPrivacy to store a consumer's preference profile in association with the consumer's account for the accessible deletion mechanism. The consumer may modify or delete the stored profile at any time. A stored preference profile shall be applied automatically to generate a prepopulated exclusion list when the consumer initiates a future deletion request through the accessible deletion mechanism. The consumer shall have the opportunity to review and adjust the resulting categorizations before submission.

12) Requires the tool to notify the consumer when a data broker previously categorized as consistent has filed an amended registration that materially changes its disclosed practices and shall prompt the consumer to review the updated categorization before the next deletion request cycle.

13) Clarifies that the privacy preference profile tool provisions do not impose obligations on registered data brokers. The tool shall operate exclusively on the basis of information data brokers are already required to disclose.

14) Provides that a data broker whose registration is found by CalPrivacy to be systematically incomplete with respect to information material to the privacy preference profile tool may be subject to enforcement for failure to make the disclosures required.

15) Requires businesses to provide an email address for consumers to submit their requests pursuant to the CCPA.

COMMENTS

1. Growth of the data broker industry

Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection provides consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of the California Constitution in 1972. Consumers' web browsing, online purchases, and involvement in loyalty programs create a treasure trove of information on consumers. Many applications on smartphones that most consumers carry with them throughout the day can track their every movement.

This information economy has given rise to the data broker industry, where the business model is built on amassing vast amounts of information through various public and private sources and packaging it for other businesses to buy. The collection of this data, combined with advanced technologies and the use of sophisticated algorithms, can create incredibly detailed and effective profiling and targeted marketing from this web of information.

Some of the largest data brokers include Experian, Equifax, TransUnion, LexisNexis, Epsilon (formerly Acxiom), and CoreLogic, as well as people-search services like Spokeo and Intelius.[1] Just one company, Epsilon, provides information on hundreds of millions of people, culled from voter records, purchasing behavior, vehicle registration, and other sources.[2]

A report by the Federal Trade Commission (FTC) found that data brokers "collect and store a vast amount of data on almost every U.S. household and commercial transaction," most of them "store all data indefinitely," and that "many of the purposes for which data brokers collect and use data pose risks to consumers."[3]

The Electronic Privacy Information Center has detailed its concerns with the secrecy and depth of the industry:

> Data brokers use secret algorithms to build profiles on every American citizen, regardless of whether the individual even knows that the data

---

[1] Barbara Booth, *What internet data brokers have on you — and how you can start to get it back* (October 11, 2024) CNBC, https://www.cnbc.com/2024/10/11/internet-data-brokers-online-privacy-personal-information.html. All internet citations are current as of April 12, 2026.
[2] Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (Mar. 19, 2018) Wired, https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.
[3] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

> broker exists. As such, consumers now face the specter of a "scored society" where they do not have access to the most basic information on how they are evaluated. The data broker industry's secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs. In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage. Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[4]

The rapidly advancing capacity of AI technology only heightens the concerns around the industry and the feeling of helplessness on the part of consumers:

> The rise of artificial intelligence tools poses the risk of even more personal information being scraped from the internet and an already opaque world of data brokering becoming even more aggressive, and that is heightening data privacy concerns. A 2023 study from Pew Research found that the American public increasingly says it does not understand what companies do with their data. According to Pew, 67% of Americans say they "understand little to nothing about what companies are doing with their personal data, up from 59% in its previous survey on the subject in 2019. A majority of Americans (73%) think they have "little to no control" over what companies do with their data.
>
> Many people are unaware that something as simple as their phone number can be used by data brokers and bad actors to uncover highly sensitive information, including a Social Security number, address, email, and even family details.… [5]

2. <u>California's data broker registry</u>

California has responded to these concerns with a number of state laws that seek to provide transparency, control, and accountability.

The CCPA, amended by the CPRA, grants a set of rights to consumers with regard to their personal information, including enhanced notice and disclosure rights regarding information collection and use practices, access to the information collected, the right to delete certain information, the right to restrict the sale of information, and protection from discrimination for exercising these rights. The CPRA also added additional protections for "sensitive personal information."

---

[4] *Data Brokers*, Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/.
[5] *See* footnote 1.

Although these are ground-breaking rights for consumers intended to protect their right to privacy, many of the provisions require consumers to know which entities have their personal information before they can properly exercise their rights. The data brokers discussed above, by definition, do not have direct relationships with consumers and can essentially amass personal information on consumers without their permission or knowledge. As found by the FTC, "because data brokers are not consumer-facing, consumers may not know where to go to exercise any choices that may be offered." The FTC report elaborated:

> Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

That FTC report further found that the attenuated connection to consumers is only further exacerbated by the fact that most data brokers obtained enormous amounts of data from other data brokers: "The data broker industry is complex, with multiple layers of data brokers providing data to each other." The FTC found that it would be "virtually impossible for a consumer to determine how a data broker obtained [their] data; the consumer would have to retrace the path of data through a series of data brokers."

To begin to address these concerns, AB 1202 (Chau, Ch. 753, Stats. 2019) established California's data broker registry. The bill was modeled on a Vermont law, Vt. Stat. Ann. tit. 9, §§ 2446 et seq., and requires data brokers to register and pay a registration fee on an annual basis.

The law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." To ensure consistency and to avoid confusion, the statute relies on existing definitions of "personal information," "third party," and "sale" in the CCPA.

Last session, SB 362 (Becker, Ch. 709, Stats. 2023) bolstered the utility and effectiveness of the data broker registry law in myriad ways and strengthened consumers' right to deletion as to data brokers by requiring the creation of an accessible deletion mechanism. SB 362 required additional information to be provided by data brokers and to be included with the other registration information on CalPrivacy's website. Data brokers are required to disclose whether and to what extent they are regulated under specified state and federal laws. This provides greater clarity for consumers on whether this especially sensitive information is being collected by a particular broker.

Last year, SB 361 (Becker, Ch. 466, Stats. 2025) again strengthened the law by, in part, requiring additional transparency from data brokers. SB 361 required a data broker to disclose whether it collects certain types of information from consumers, including consumers' citizenship data, immigration status, union membership status, sexual orientation status, or biometric data. Given the sensitive nature of much of this information and the increasing hostility from the federal government and other states toward certain populations, these disclosures provide consumers with valuable insight into which brokers maintain this type of information.

3. Enhancing the laws regulating data brokers

This bill again bolsters the data broker registry law by requiring additional transparency from data brokers. Building off the legislation above, the bill dives deeper into the inner workings of data brokers but requires them to disclose whether they take certain forms of information, including citizenship data, sexual orientation, and union membership, and sell inferences about the attributes of a consumer based on their analysis of that data. This transparency provides additional pieces of the puzzle for consumers to more fully understand what is being done with their information.

Next, the bill codifies existing CalPrivacy regulations by importing the definition of "direct relationship" as that term is used in the definition of data broker. Currently, "data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a *direct relationship*. Drawing from the relevant regulations, the bill now inserts a definition of "direct relationship" to mean that a consumer has intentionally interacted with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services. It requires a consumer to intend to interact with the business and the threshold is not met simply because a business collects personal information directly from the consumer. In addition, a business does not have a "direct relationship" with a consumer as to personal information it sells about the consumer that it collected outside of a first-party interaction with the consumer. The language imported does not directly line up with that regulation, however. The author has agreed to amendments that bring the language of the bill into tighter alignment.

Finally, the bill requires CalPrivacy, as part of the accessible deletion mechanism currently known as DROP (Delete Request and Opt-out Platform), to create a "privacy preference profile tool." The tool must allow consumers to detail their privacy preferences regarding data broker data collection and use practices. CalPrivacy is required to categorize each data broker in one of three categories based on the broker's most recent annual registration disclosure. Data brokers can be "consistent," their practices are compatible with the consumer's preferences, or "inconsistent," where the practices conflict with any of the consumer's preferences. If the data broker's registration is "silent, ambiguous, or incomplete with respect to a profile dimension that

is material to the consumer's preferences," the broker must be listed as "indeterminate." In the latter case, the tool shall display the specific gap in disclosure that produced this categorization.

The tool must then display the list of all registered data brokers broken down by the three categories prior to the consumer's submission of a deletion request through DROP.

In summary, CalPrivacy must analyze each data broker's privacy practices to determine whether they match up with the preferences expressed by each consumer electing to use the tool. They must also provide an explanation to each consumer about why any data broker is listed as indeterminate, which means a broker's registration was not clear with respect to a "profile dimension that is material" to the consumer. The self-reported practices of the data brokers is the source of information from which these determinations will be made.

This mechanism presupposes that consumers are looking for and derive benefit from continuing to allow some data brokers to collect, maintain, and sell their personal information, despite not having a direct relationship with the consumer. Existing law already allows a consumer to selectively exclude specific data brokers from a deletion request and provides the ability for data brokers to include in their registration any additional information or explanation the data broker chooses to provide concerning its data collection practices from which consumers can inform their decisions. Having CalPrivacy identify certain data brokers as "consistent" with a consumer's stated preferences may also lead to confusion and overreliance on the part of consumers regarding the benefit provided consumers by excluding such data brokers from a deletion request. In response the author has agreed to remove these provisions of the bill. Instead, the amendment will direct the Office of Data and Innovation to create such a tool that may be used by agencies, including CalPrivacy.

According to the author:

> California led the nation with the Delete Act, giving consumers the power to request that data brokers delete their personal information through a single mechanism. SB 1104 builds on that foundation.
>
> Today, data brokers can avoid the "data broker" label by claiming a direct relationship with consumers they have never meaningfully interacted with. Others avoid transparency requirements by selling inferences drawn from sensitive data rather than collecting it directly, profiling a consumer's reproductive health or immigration status without ever disclosing that activity. SB 1104 closes these gaps with clear definitions and new disclosure requirements.

> Finally, the bill directs the California Privacy Protection Agency to build a privacy preference profile tool that puts consumers at the center. Rather than forcing Californians to navigate a complex and opaque data ecosystem on their own, the tool empowers Californians to understand what data brokers are collecting, how their personal information is being used, and which brokers align with their own privacy values. It is a human centered approach that gives consumers not just the power to delete their data but the clarity to make informed decisions about when and how to use that power.

SUPPORT

None received

OPPOSITION

None received

RELATED LEGISLATION

SB 923 (Becker, 2026) expands consumers' right to deletion of their personal information pursuant to the CCPA and requires specified online businesses to provide consumers an online method for exercising rights under the CCPA. SB 923 is currently in the Senate Appropriations Committee.

SB 1106 (Cabaldon, 2026) shortens the timelines within which a data broker must comply with various provisions within the Delete Act. SB 1106 is currently in the Senate Appropriations Committee.

SB 361 (Becker, Ch. 466, Stats. 2025) *See* Comment 2.

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

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.

AB 1202 (Chau, Ch. 753, Stats. 2019) *See* Comment 2.

SB 1348 (DeSaulnier, 2014) would have required a data broker, as defined, that sells or offers for sale to a third party the personal information of any resident of California, to permit an individual to review their personal information and demand that such information not be shared with or sold to a third party. It would have provided consumers with their own enforcement mechanism to hold data brokers in violation

accountable. This bill was held in the Assembly Arts, Entertainment, Sports, Tourism, and Internet Media Committee.

****