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

SB 361 (Becker)
Version: March 24, 2025
Hearing Date: April 1, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Data broker registration: data collection

DIGEST

This bill expands the disclosures that data brokers must make when registering with California's Data Broker Registry.

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 and more fully inform consumers about who is collecting their personal information and how, California established a data broker registry, requiring data brokers to register annually with the Attorney General. Data brokers are required to pay a fee and provide certain information about their location, email, and website addresses. Recent updates have bolstered the law to provide consumers more control over their information, by, in part, requiring more information to be reported, including an annual report from data brokers on their compliance with California Consumer Privacy Act (CCPA) requests, increasing penalties for violations, and transferring much of the relevant duties from the Attorney General to the Privacy Protection Agency (PPA). It also expanded consumers' deletion rights and requires the PPA to create an accessible deletion mechanism. This bill again fortifies the law by requiring additional disclosures from data brokers on the types of information collected. This bill is sponsored by Oakland Privacy and supported by a number of organizations. No timely 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 the PPA, 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) Aligns the definitions of "business," "personal information," "sale," "collect," "consumer," and "third party" with those in the CCPA. (Civ. Code § 1798.99.80.)

4) Requires data brokers to provide, and the PPA 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.)

5) 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.)

6) 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.)

7) 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.)

8) 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.)

9) Establishes the California Privacy Rights Act of 2020 (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).)

10) 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).)

11) 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).)

12) 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.)

13) 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.)

14) 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 the sale or sharing of their personal information. (Civ. Code § 1798.120.)

15) Provides that these provisions do not restrict a business' ability to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information. (Civ. Code § 1798.145(a)(6).)

16) 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).)

17) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information

such as genetic data and the processing of biometric information for the purpose of uniquely identifying a consumer. (Civ. Code § 1798.140(ae).)

18) 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.)

19) 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 data brokers registering with the CPPA to indicate whether they collect the following information on consumers:
    a) account login or account number in combination with any required security code, access code, or password that would permit access to a consumer's account with a third party;
    b) drivers' license number, California identification card number, tax identification number, social security number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
    c) citizenship data, including immigration status;
    d) union membership status;
    e) sexual orientation status; or
    f) biometric data.

2) Provides that the Legislature finds and declares that this act advances the purposes and intent of the California Privacy Rights Act of 2020 by strengthening the constitutional right to privacy and safeguarding consumers' rights. To achieve this, the act expands disclosure requirements for data brokers, thereby enhancing transparency for consumers.

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 the 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 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

[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 March 17, 2025.
[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.

> 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. California's data broker registry

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 in additional protections for "sensitive personal information."

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,

---

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

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."

The FTC report is entitled "Data Brokers: A Call for Transparency and Accountability," and it specifically called for a robust legislative response:

> Many of these findings point to a fundamental lack of transparency about data broker industry practices. Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge.
>
> In light of these findings, the Commission unanimously renews its call for Congress to consider enacting legislation that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities.

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 the PPA'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.

3. Enhancing the data broker registry law

This bill bolsters the data broker registry law by requiring additional transparency from data brokers. The bill requires a data broker to disclose whether it collects certain types of information from consumers, including consumers' citizenship data, including 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. For instance, it has widely been reported that government 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."[6]

These new disclosure requirements build on those imposed by SB 362, namely the obligation for data brokers to indicate whether they collect personal information from minors or the precise geolocation or reproductive health care data of consumers. This type of transparency is crucial as existing regulations do not require data brokers to notify consumers at the point personal information is being collected from them because there is no direct relationship as with other businesses.

According to the author:

> Californians have a right to know who is collecting their most sensitive personal information. SB 361 increases transparency in the data broker industry, helping people protect their privacy.
>
> There are serious concerns that data brokers are selling sensitive information in ways that could lead to surveillance and targeting of vulnerable communities, including immigrants, and LGBTQ+ individuals.

[6] 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.

> The risks of mass deportation, discrimination, and other harmful outcomes are real, and we must act to protect people's privacy.
>
> Building on the California Delete Act, which was passed in 2023, SB 361 requires data brokers to disclose whether they collect sensitive information like government IDs, union membership, and sexual orientation. The California Privacy Protection Agency (CPPA) will publish this information, empowering Californians to make informed decisions about their privacy and will soon have the ability with the click of a single link to delete their personal data and prevent it from being sold.
>
> California has long been a leader in privacy protections, and SB 361 ensures that individuals—not data brokers—remain in control of their personal information.

Oakland Privacy, the sponsor of the bill, writes:

> While Californians generally have concerns about third party selling of any of their personal information, when the information is highly sensitive those concerns are, most reasonably, greatly increased. It is also fair to say that recent developments on the federal side have amplified those concerns as Californians have watched federal databases containing some highly personal data about them be breached by unauthorized personnel for unclear purposes.
>
> The premise of SB 361 is that Californians have a right to know which companies have obtained and are prepared to sell their highly sensitive information and to be able to distinguish those particular data brokers from those who are distributing less sensitive information. We absolutely agree that both consumers and regulators should have access to this information, and most importantly, that gaining that access should not be a burdensome process for consumers.

SUPPORT

Oakland Privacy (sponsor)
California Federation of Labor Unions, AFL-CIO
Consumer Reports
Electronic Privacy Information Center
Privacy Rights Clearinghouse
Puente de la Costa Sur

OPPOSITION

None received

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

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.

****