SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 362 (Becker)
Version: April 10, 2023
Hearing Date: April 25, 2023
Fiscal: Yes
Urgency: No
CK

SUBJECT

Data brokers: registration

DIGEST

This bill enhances the data broker registry law and transfers most of the attendant duties from the Attorney General to the California Privacy Protection Agency.

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, a data broker registry was established in California law 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. Responding to concerns that existing law does not do enough to bring this industry into the light and to provide consumers more control over their personal information, this bill bolsters the data broker registry law by, in part, requiring more information to be reported, including an annual report from data brokers on their compliance with CCPA/CPRA requests, increasing the penalties for violations, and transferring much of the relevant duties from the Attorney General to the California Privacy Protection Agency (PPA). It also expands 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.

This bill is sponsored by Privacy Rights Clearinghouse. It is supported by a variety of consumer and privacy rights organizations, including Consumer Action and the Electronic Frontier Foundation. It is opposed by various industry groups, including the Consumer Data Industry Association.

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 Attorney General, 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) a consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
    b) a financial institution 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 pay a registration fee in an amount determined by the Attorney General, not to exceed the reasonable costs of establishing and maintaining the informational Internet Web site that this bill requires the Attorney General to create and make accessible to the public. (Civ. Code § 1798.99.82.)

5) Requires data brokers to provide, and the Attorney General to include on its Web site, the name of the data broker and its primary physical, email, and Internet Web site addresses. Data brokers may, at their discretion, also provide additional information concerning their data collection practices. (Civ. Code §§ 1798.99.82, 1798.99.84.)

6) Subjects a data broker that fails to register as required by this section to injunction and civil penalties, fees, and costs to be recovered in an action brought in the name of the people of the State of California by the Attorney General. The

remedies include civil penalties of $100 for each day the data broker fails to register; a monetary award in an amount equal to the fees that were due during the period it failed to register; and expenses incurred by the Attorney General in the investigation and prosecution of the action as the court deems appropriate. (Civ. Code § 1798.99.82.)

7) Provides that any penalties, fees, and expenses recovered in such actions are to be deposited in the Consumer Privacy Fund, to be used to fully offset the relevant costs incurred by the state courts and the Attorney General. (Civ. Code §§ 1798.99.81, 1798.99.82.)

8) Provides that the above shall not supersede or interfere with the operation of the California Consumer Privacy Act (CCPA). (Civ. Code § 1798.99.88.)

9) 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.)

10) 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).)

11) 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).)

12) Provides that a business or service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business or service provider to maintain the consumer's personal information in order to do certain things, including to comply with a legal obligation. (Civ. Code § 1798.105(d).)

13) 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).)

14) 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 or selling 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.)

15) Provides consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer the following:
    a) the categories of personal information that the business collected about the consumer;
    b) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
    c) the categories of personal information that the business disclosed about the consumer for a business purpose. (Civ. Code § 1798.115.)

16) 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.)

17) 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).)

18) 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).)

19) 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).)

20) 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.)

21) 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) Transfers the relevant duties of the Attorney General in the data broker registry law to the California Privacy Protection Agency. It authorizes actions to be brought against data brokers in violation of the law by either the Attorney General or the PPA and increases the civil penalty to $200.

2) Updates definitions to cross-reference to the CPRA.

3) Allows for funds in the "Data Broker's Registry Fund," which shall include any monies recovered in an action pursuant to the data broker registry law, to be used to offset certain costs, including enforcement costs and any costs associated with creating and maintaining the deletion mechanism.
4) Requires data brokers, when registering, to additionally provide various additional pieces of information, including:
    a) whether the data broker collects data of minors; precise geolocation data; or reproductive health care data; and
    b) a link to a website that includes details on how consumers may exercise their rights to delete personal information, correct inaccurate personal information, know what personal information is being collected, sold, or shared, and how to access it, how to opt-out of the sale or sharing of personal information, and how to limit the use and disclosure of sensitive personal information.

5) Requires data brokers to compile and report certain metrics related to CCPA compliance.

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 PI related to the consumer, as specified. Data brokers are required to regularly access the mechanism and process requests for deletion.

7) Prohibits a data broker from collecting, retaining, selling, or sharing PI of a consumer who has submitted a deletion request unless the data collection is requested by the consumer.

8) Requires data brokers to undergo audits every three years to determine compliance with the data broker registry law.

9) Authorizes the PPA to adopt regulations in compliance with the Administrative Procedure Act.

10) Provides that the Legislature finds and declares that this act furthers the purposes and intent of the CPRA by ensuring consumers' rights, including the constitutional right to privacy, are protected by enabling and empowering Californians to request that data brokers delete their personal information and prohibiting data brokers from collecting consumers' personal information in the future.

COMMENTS

1. Protecting the fundamental right to privacy

Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Privacy is therefore not just a policy goal; it is a constitutional right of every Californian. However, it has been under increasing assault.

The phrase "and privacy" was added to the California Constitution as a result of Proposition 11 in 1972; it was known as the "Privacy Initiative." The arguments in favor of the amendment were written by Assemblymember Kenneth Cory and Senator George Moscone. The ballot pamphlet stated, in relevant part:

> At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian. The right of privacy . . . prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. . . . The proliferation of government and business records over which we have no control limits our ability to control our personal lives. . . . Even more dangerous is the loss of control over the accuracy of government and business records on individuals. . . . Even if the existence of this information is known, few government agencies or private businesses permit individuals to review their files and correct errors. . . . Each time we apply for a credit card or a life insurance policy, file a tax return, interview for a job[,] or get a drivers' license, a dossier is opened and an informational profile is sketched.[1]

In 1977, the Legislature reaffirmed that the right of privacy is a "personal and fundamental right" and that "all individuals have a right of privacy in information pertaining to them." (Civ. Code § 1798.1.) The Legislature further stated the following findings:

- "The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."
- "The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."

---

[1] *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 17, quoting the official ballot pamphlet for the Privacy Initiative.

- "In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

Although written almost 50 years ago, these concerns seem strikingly prescient.

2. 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. 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.

A leader in this industry is Acxiom, a data broker that provides information on hundreds of millions of people, culled from voter records, purchasing behavior, vehicle registration, and other sources.[2] Acxiom offers "the most accurate and comprehensive consumer insights and data" with data on 250 million U.S. consumers, or approximately 75 percent of the country's population.[3] It boasts that its "full scope of data and insights covers the globe with reach of 2.5 billion addressable consumers." The company provides a sketch of the data elements collected: individual demographics such as age, gender, ethnicity, education; number/ages of children; economic stability; marriage/divorce; birth of children; products bought; and behavioral details, including community involvement, causes, and gaming.

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

---

[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/. All internet citations are current as of April 7, 2023.
[3] *ACXIOM DATA: Unparalleled Global Consumer Insights*, Acxiom, https://www.acxiom.com/wp-content/uploads/2019/02/Acxiom_Data_Overview_2019_02.pdf.

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."[4]

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 brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[5]

Consumers have expressed growing concern in response to this profiling. A study by the Pew Research Center found that 68 percent of American Internet users believe existing law does not go far enough to protect individual online privacy, with only 24 percent believing current laws provide reasonable protections.[6]

3. 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 to protect their right to privacy, many of the provisions require consumers to know which entities have their

---

[4] 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.
[5] *Data Brokers*, Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/.
[6] Lee Rainie et al., *Anonymity, Privacy, and Security Online* (Sep. 5, 2013) Pew Research Center, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

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."

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 with, and pay a registration fee to, the Attorney General 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 cross-

references to the definitions of "personal information," "third party," and "sale" in the CCPA.

Data brokers are only required to report their name and primary physical, email, and internet website addresses. They have the option to provide additional information or explanation regarding their data collection practices, but this is not required. The Attorney General must then post this information online so that it is accessible to consumers.

To encourage compliance, the law provides for modest civil penalties, $100 per day, for failing to register, as well as injunctive relief. Such penalties, along with fees and expenses, are only available in an action brought by the Attorney General.

4. Enhancing the data broker registry law

According to the author:

> In today's digital age, our personal information is constantly being collected, sold, and shared by data brokers without our knowledge or consent. These entities build extensive profiles on individuals, amassing often sensitive information ranging from browsing history to financial records, social media activity, precise geolocation information and even reproductive healthcare data.
>
> With increased criminalization of abortion and gender affirming care occurring nationwide, the potential misuse of healthcare data could lead to harassment, discrimination, and even legal consequences for those who seek those services in California. Elderly individuals are at a higher risk for scams, identity theft, and financial exploitation that rely on the collection and misuse of personal information. Without adequate knowledge about the types of information collected and sold by data brokers, and without the ability to delete that information upon request, consumers are left defenseless against such practices and suffer from diminished autonomy and privacy in their daily lives.
>
> While California has taken steps to require data brokers to register with the Attorney General, our existing frameworks fall short of providing the necessary tools for individuals to protect their privacy. Currently, the data broker registry is impractical because it requires Californians to request each of the more than five-hundred registered brokers to delete their personal information, a practically impossible task for all but the most concerned consumers. Those that do attempt to delete their information using the data broker registry will find that the Right to Delete under the California Consumer Privacy Act is limited to information "collected from

> the consumer" and doesn't cover most of the information that a data broker will possess.
>
> SB 362 seeks to address these concerns by creating a user-friendly webpage within the California Privacy Protection Agency where all Californians can delete their information from data brokers free of charge. The bill also strengthens our privacy rights by requiring data brokers to report what information they collect on us and mandating deletion of that information upon request. By making data brokers more transparent and accountable, we can better protect ourselves against potential misuse of our data and exercise our privacy rights.
>
> These changes are critical to better safeguarding Californians' privacy and well-being in the digital age. By enhancing transparency and giving consumers more control over their data, SB 362 represents an important step forward in protecting our privacy rights.

This bill bolsters the utility and effectiveness of the existing data broker registry law in myriad ways and strengthens consumers' right to deletion as to data brokers.

First, the bill transfers most of the responsibilities for the registry from the Attorney General to the PPA. Data brokers will register with, and all information will be reported to, the PPA, which will then post the relevant information on their website.

Both the Attorney General and the PPA will be authorized to enforce violations of the law, as provided, and to collect increased penalties and fines, in addition to expenses incurred by the prosecuting entity. Monies collected are to be deposited into the Data Brokers' Registry Fund, which the bill establishes in the State Treasury, in lieu of the Consumer Privacy Fund.

Secondly, the bill also updates the definitions section to simply cross reference to the definitions in the CCPA/CPRA, except as otherwise specified.

Third, it requires 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. It will also require data brokers to disclose whether they collect PI from children and whether they collect consumers' precise geolocation or reproductive health care data. This provides greater clarity for consumers on whether this especially sensitive information is being collected by a particular broker.

Data brokers must also provide a link to a page on the data broker's internet website that details how consumers can exercise their CPRA rights, including how to: learn what personal information is being collected; access that PI; delete their PI; correct

inaccurate PI; learn what PI is being sold or shared, and to whom; learn how to opt out of the sale or sharing of PI; and limit the use and disclosure of sensitive PI. The site is explicitly restricted from making use of dark patterns.

Ready access to this information is crucial as existing regulations do not require data brokers to notify consumers at the point PI is being collected from them because there is no direct relationship as with other businesses.

Data brokers are also required to submit new metrics that are compiled on an annual basis. This includes the number of CPRA requests received, complied with, and denied, and the attendant timelines for responding to those requests. This information is required to be posted with registration information on the PPA website. This information is also required to be posted on a data broker's website with information about the bases for denying requests. A link to this page must be provided in the data broker's privacy policy. This provides a new layer of transparency to this largely opaque industry.

Fourth, the bill requires the PPA to establish an "accessible deletion mechanism" that is capable of doing both of the following:

- implementing and maintaining reasonable security procedures and practices, including, but not limited to, administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the PI will be used and to protect consumers' PI from unauthorized use, disclosure, access, destruction, or modification; and
- allowing a consumer, through a single verifiable consumer request, to request that every data broker that maintains any PI delete any PI related to that consumer held by the data broker or associated service provider or contractor.

The bill prescribes specific requirements for the system, including security and accessibility standards. The PPA is authorized to promulgate regulations as necessary to improve the operational privacy and security of the mechanism and the system for accessing it.

Data brokers are required to access the system securely on an at least monthly basis and process all pending deletion requests. They are further required to direct their service providers or contractors to also delete all such PI.

A mechanism of this sort provides a much greater degree of control to consumers over their PI. First, it is largely impractical for a consumer to navigate the systems of the hundreds of data brokers and to submit deletion requests individually to each. This allows a consumer to delete their information with a single, secure request. But more importantly, this greatly expands the right from the deletion rights provided under the CPRA. Under the CPRA, a consumer has the right to request that a business delete any

PI about the consumer which the business has *collected from the consumer*. The bill now provides for the creation of a mechanism that allows a consumer to request a data broker delete ALL of the PI the data broker has that relates to the consumer, regardless of its source. (Civ. Code § 1798.105.) Just as with the CPRA, there are exceptions allowing for brokers to retain PI where necessary, for instance, to comply with a warrant or other applicable law or for the exercise of free speech.

The author argues that the existing right to delete is ineffectual when applied to information in the hands of data brokers, as they do not collect the information directly. The author asserts that this creates a "loophole that leaves Californians vulnerable to the risks associated with unauthorized data collection and sale."

The bill goes even further and prohibits a data broker from collecting, retaining, selling, or sharing any PI of a consumer who has previously submitted a deletion request, unless thereafter being requested by the consumer. No such right to prohibit the collection of PI currently exists.

Finally, the bill requires, starting in 2027, data brokers to undergo an audit by an independent third party to determine compliance with the data registry law and to submit it the PPA.

This bill is modeled after bipartisan federal legislation, the Data Elimination and Limiting Extensive Tracking and Exchange (DELETE) Act, introduced by Senators Jon Ossoff and Bill Cassidy, with a companion bill introduced by Representative Lori Trahan in the House of Representatives. The members state their reasoning.

> Senator Ossoff: "Data brokers are buying, collecting, and reselling vast amounts of personal information about all of us without our consent. This bipartisan bill is about returning control of our personal data to us, the American people."
>
> Senator Cassidy: "People expect privacy and their personal information to be protected. This bill gives Americans a solution to ensure their personal data is not tracked, collected, bought or sold by data brokers."
>
> Congresswoman Lori Trahan: "Americans across the political spectrum agree that online companies have nearly total control of the data collected on them, and they're right. Once our phone number, web history, or even social security number gets added to a data broker's list, it becomes nearly impossible to get it removed. I'm proud to introduce the bipartisan DELETE Act to return power

> back to consumers by giving each of us the right to have sensitive personal information removed from these lists."[7]

Privacy Rights Clearinghouse, the sponsor of the bill, writes:

> Currently, the Data Broker Registry is impractical, requiring Californians to individually exercise their privacy rights with each of the more than five-hundred registered brokers. Further, data brokers are not required to disclose what kind of information they collect from consumers. The current deletion process is time-consuming and practically impossible for even the most dedicated consumers, but especially for those with limited access to technology or facing language barriers. As a result, Californians are left unable to effectively protect their privacy and exercise their rights.
>
> **Solution**
> SB 362 seeks to address these concerns by creating a user-friendly webpage within the California Privacy Protection Agency where all Californians can delete their information from data brokers free of charge. The bill also strengthens consumer privacy rights by requiring data brokers to report what information they collect on us – including when, for example, the data broker collects reproductive healthcare information or precise geolocation information - and mandating deletion of that information upon request. By making data brokers more transparent and accountable, we can better protect ourselves against potential misuse of our data and exercise our privacy rights.
>
> By enhancing transparency and giving consumers control over their data, this bill will help protect Californians' privacy and mitigate the risks associated with the collection and sale of sensitive personal information by data brokers. By enhancing transparency and giving consumers more control over their data, SB 362 represents an important step forward in protecting our privacy rights.

5. Furthering the purpose and intent of the CPRA

Section 25 of the CPRA, passed by voters in November 2020, 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

---

[7] *Sens. Ossoff & Cassidy Introduce Bipartisan Legislation to Give Americans Control of Their Online Data* (February 10, 2022) Senator Jon Ossoff webpage, https://www.ossoff.senate.gov/press-releases/sens-ossoff-cassidy-introduce-bipartisan-legislation-to-give-americans-control-of-their-online-data/.

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.

The section also lays out various guiding principles about how the law should be implemented. The bill explicitly states:

> The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020 by ensuring consumers' rights, including the constitutional right to privacy, are protected by enabling and empowering Californians to request that data brokers delete their personal information and prohibiting data brokers from collecting consumers' personal information in the future.

Although not amending the CPRA itself, the bill impacts privacy and clearly operates in the same regulatory space. The bill enhances the data registry law, bolstering its utility in keeping consumers informed of where their information goes and what they can do with it. Therefore, the bill arguably furthers the purposes and intent of the CPRA.

6. Stakeholder positions

A coalition of consumer and privacy rights groups, including the California Association for Micro Enterprise Opportunity and Electronic Frontier Foundation, write in support:

> In today's digital age, our personal information is constantly being collected, sold, and shared by data brokers without our knowledge or consent. These entities build extensive profiles on individuals, amassing oftentimes sensitive information ranging from browsing history to financial records, social media activity, precise geolocation information, and even reproductive healthcare data.
>
> These concerns are not abstract for countless Californians. With increased criminalization of abortion and gender affirming care occurring

> nationwide, the potential misuse of healthcare data could lead to harassment, discrimination, and even legal consequences for those who seek those services in California. Elderly individuals are at a higher risk for scams, identity theft, and financial exploitation that rely on the collection and misuse of personal information. Furthermore, invasive marketing practices and price discrimination can result from data brokers' sale of consumer information to businesses. Without adequate knowledge about the types of information collected and sold by data brokers, and without the ability to delete that information upon request, consumers are left defenseless against such practices, and suffer from diminished autonomy and privacy in their daily lives.
>
> While California has taken steps to require data brokers to register with the Attorney General, our existing frameworks fall short of providing the necessary tools for individuals to protect their privacy. Though the California Consumer Privacy Act empowers individuals with a "Right to Delete" information from businesses that collect their personal information, that right is limited to that collected "from the consumer." Data brokers do not collect information from consumers directly, creating a loophole that leaves Californians unable to exercise this essential right and vulnerable to the risks associated with unauthorized collection, sale, and misuse.

Writing in opposition, an advertising industry coalition, including the Digital Advertising Alliance, argue:

> The bill would create data broker transparency provisions that do not take into account similar provisions in the CCPA. The bill would, for example, require data brokers to provide metrics regarding consumer requests as well as information regarding personal information collection and disclosure practices. The bill also directs the CPPA to "create a page on its internet website where the registration information provided by data brokers… shall be accessible to the public." The CCPA itself creates similar requirements for the data brokers it covers by requiring such disclosures through privacy policies. As a result, the requirements in SB 362 are at least duplicative of, and may even conflict with, information disclosures currently mandated under California law.
>
> In addition, the bill would require the Agency to "establish an accessible deletion mechanism that…[a]llows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor." This data broker deletion mechanism would rob consumers of

> the ability to elect not to do business with certain data brokers while choosing to engage with others. Such an overly broad deletion mechanism would serve as a very blunt instrument that would not provide consumers with the ability to make granular choices. Consumers should be permitted to set specific preferences regarding data brokers' ability to process personal information rather than be forced into making all-or-nothing decisions.

The California Chamber of Commerce writes in opposition:

> What consumers need is to know who these companies are, how to access the same privacy disclosures that they could access from any other business that they might have a direct relationship with, and how to initiate CCPA requests, the same as they would with other businesses – things that are already done by the existing repository created in AB 1202.
>
> Data brokers provide services to many other businesses in support of anti-money laundering, sanction compliance, cybersecurity, and underwriting activities. Creating duplicative and conflicting reporting requirements and deletion obligations not only creates unnecessary work and increases the chances of mistakes being made, but it also can undermine these legitimate and necessary functions.
>
> Lastly, establishing new and major responsibilities for the CPPA is not only unnecessary as illustrated above, but concerning given how far behind the CPPA currently is on issuing full and final regulations implementing the CCPA as it was amended by Proposition 24 in 2020.

Concerns have also been raised by opposition regarding the strict prohibition on collecting and retaining personal information after a consumer has submitted a deletion request. They argue it is unworkable and should instead simply restrict use or sharing. In response, the author has agreed to amendments that allow for collection and retention after a deletion request has been processed, but require the data broker to delete any new personal information that comes in on the consumer no less frequent than 31 days.

SUPPORT

Privacy Rights Clearinghouse (sponsor)
Calegislation
California Association for Micro Enterprise Opportunity
CALPIRG
Consumer Action
Consumer Federation of America

Consumer Reports
Electronic Frontier Foundation
Fairplay
Oakland Privacy
Ultraviolet Action

OPPOSITION

American Advertising Federation
American Association of Advertising Agencies
Association of National Advertisers
Better Identity Coalition
California Bankers Association
California Chamber of Commerce
California Financial Services Association
California Retailers Association
Consumer Data Industry Association
Digital Advertising Alliance
Insights Association
Software & Information Industry Association
State Privacy and Security Coalition
TechNet

RELATED LEGISLATION

Pending Legislation:

AB 1546 (Gabriel, 2023) extends the statute of limitations for actions to enforce the CCPA by the Attorney General to five years. AB 1546 is currently in the Assembly Judiciary Committee.

AB 947 (Gabriel, 2023) adds citizenship or immigration status to the definition of "sensitive personal information" in the CCPA, affording it greater protections. AB 947 is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

SB 1059 (Becker, 2022) would have enhanced the data broker registry law and transfers most of the relevant duties from the Attorney General to the California Privacy Protection Agency.

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.

****