SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

SB 1059 (Becker)
Version: March 7, 2022
Hearing Date: April 19, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Privacy: data brokers

DIGEST

This bill enhances the data broker registry law and transfers most of the relevant 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. The data brokers are required to pay a fee and provide certain information about their location, email, and internet 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 expands the definition of data broker, requires more information to be reported, increases the civil penalties for violations, and transfers much of the relevant duties from the Attorney General to the California Privacy Protection Agency (PPA).

This bill is sponsored by the author. It is supported by a variety of consumer and privacy rights organizations, including Consumer Reports. It is opposed by a coalition of industry groups, led by the California Chamber of Commerce.

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 definitions 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 (Ins. 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) 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 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.)

13) 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.)

14) Provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold and that consumers have the right to opt out of the sale 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." (Civ. Code § 1798.140(v)(1).)

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) 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 cross references to the CPRA for various definitions and adds new references for "sensitive personal information" and "shares."

3) Includes within the definition of "data broker" the sharing of personal information with third parties.

4) Requires data brokers, when registering, to additionally provide the following information:
    a) whether the data broker has been breached and, if yes, additional details of each breach;
    b) whether the data broker collects data of minors; and
    c) instructions 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 the PPA, on or before January 1, 2024, to adopt regulations in compliance with the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code) to further the purposes of the data broker registry law.

6) 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 centralizing privacy rights enforcement with the PPA.

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."

---

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

- "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."
- "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 consumers' 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.

---

[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 4, 2022.
[3] *ACXIOM DATA: Unparalleled Global Consumer Insights*, Acxiom, https://www.acxiom.com/wp-content/uploads/2019/02/Acxiom_Data_Overview_2019_02.pdf.

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."[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."

---

[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/.

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 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:

> Just because we live and work in the Digital Age does not mean we waive our rights to privacy. Our personal information is a prized commodity for data brokers, which are entities that collect, sell, and share our personal information even though they do not have a direct business relationship with us. Brokers provide third parties the means to profile and target us for ads, sales pitches and other content, and to follow our behavior, including tracking us in real time to specific locations. The breadth of information data brokers acquire is staggering.
>
> SB 1059 will better protect Californians from potential misuse of our personal data and shine a stronger light on data brokers and their activities. The bill strengthens privacy rights and forces data brokers to be more transparent by requiring them to provide clear instructions on how consumers can delete, correct, opt-out, or identify who has purchased their personal data, and how to limit the use of our sensitive personal information. The bill also requires data brokers to disclose to the public if they have been breached and if they collect, sell, or share information regarding children. These and other changes in SB 1059 are designed to better protect against the potential misuse of our data and strengthen Californians' ability to exercise their privacy rights.

This bill bolsters the utility and effectiveness of the existing data broker registry law in several ways. First, it requires additional information to be provided by data brokers and to be included in the registry. This will include instructions on how consumers can

exercise their rights under the CCPA/CPRA. It will also require data brokers to disclose whether they collect children's information and whether they have been breached. If they have been breached, they are required to provide more detailed information.

Writing in opposition, a California Chamber of Commerce-led coalition raises concerns:

> SB 1059 seeks to have businesses on the Data Broker Registry disclose whether they have been breached and, if so, provide additional details of each breach. The bill, however, provides no definition as to what constitutes a data breach and provides constraints on how far a business must reach back into its history for reporting purposes. If anything, the bill should be limited to breaches that were subject to notice to the AG under [California's Data Breach Notification Law], or otherwise rely on a definition of data breach that is consistent with existing law, and it should be time limited to ensure that only recent and relevant breaches are captured. Without such guardrails, even inadvertent access to encrypted personal information that did not result in any disclosure or use by an unauthorized individual over 20 years ago could become reportable on the Data Broker Registry.

In response to these concerns, the author has agreed to include a definition of "data breach" that is tied to California's Data Breach Notification Law.

> Amendment
>
> Insert cross-reference to Civil Code section 1798.82(g) for the definition of data breach

Secondly, the bill transfers most of the responsibilities for the registry from the Attorney General to the PPA. All information will be reported to the PPA, which will then post it on their website. The PPA is also tasked with promulgating regulations to carry out its duties pursuant to the updated law by January 1, 2024. The intent is to house the oversight of California's premier privacy laws within one agency, focused solely on these issues.

The opposition coalition argues:

> As the business community anxiously awaits the delayed CPRA regulations that are critical to compliance efforts, we urge the Legislature to allow the CPPA to focus on its primary functions in issuing those regulations and overseeing the implementation [of] the privacy act. Even still, we believe it is one thing to transfer the Data Broker Registry from the [Attorney General (AG)] to the CPPA; it is another to require the CPPA to issue new regulations just as the CPRA starts to take effect.

> To be clear, the only regulation set forth by the AG for the Data Broker Registry pertains to the amount of the registration fee. While updates to that fee may be appropriate in the future, certainly, the CPPA does not need to be required to issue regulations by a date certain to do so. Requiring regulations by January 1, 2024, effectively eliminates the Agency's ability to exercise any discretion around whether an increase is appropriate or necessary.

In response to these concerns, the author has agreed to remove the date by which the PPA must issue regulations.

> Amendment
>
> Remove "On or before January 1, 2024" from Section 1798.99.85.

While the bill authorizes the PPA to initiate action against data brokers in violation of the law, it preserves the right of the Attorney General to also enforce its provisions. As for those actions, the bill increases the modest civil penalty to $200 for each day the data broker fails to register as required.

Finally, the bill also updates cross references to the definitions in the CCPA/CPRA and includes additional terms introduced by the CPRA, such as the category of "sensitive personal information." It also includes a reference to "sharing" as understood in the CPRA. The definition of data broker is likewise expanded to include businesses that share personal information with third parties that relates to consumers the business does not have a direct relationship with. Highlighting the importance of this change, Consumer Reports (CR) indicates that they have "found that some companies have sought to avoid the CCPA's opt out by claiming that much online data sharing is not technically a 'sale.'" The CPRA expanded the scope of California's opt-out to include all data *sharing*. Therefore, a similar expansion makes sense in this law, to better ensure that all data brokers are required to register.

CR's letter continues:

> Data brokers buy and sell consumer information, almost always without the consumers' knowledge. In 2019, CR supported the creation of a public, mandatory data broker registry to help bring these businesses out of the shadows, and to make it easier for consumers to exercise their privacy rights under the California Consumer Privacy Act (CCPA) with respect to these companies. Now, we recommend updating the data broker registry through SB 1059, to ensure consistency with the CCPA as amended by Proposition 24, and to better ensure that the registry works for consumers.

> Some data brokers, such as Acxiom and Intelius, collect personal details about consumers' behavior online, their income, and addresses, which is used to create a detailed profile about them. This information is then sold and resold, and often used for marketing and potentially for other purposes. Without an effective data broker registry, consumers would have limited ability to identify which data brokers are selling their personal information, or how to contact them. [footnotes omitted]

The opposition coalition writes:

> In requiring registered data brokers to provide additional information in their registrations, SB 1059 is, at best, redundant in requiring the provision of information that is already available to consumers. At worst, the utility of the Registry will almost surely be reduced by requiring the registration of businesses that are not data brokers and requiring additional information to be provided by each of those businesses, making it more difficult for consumers to find relevant information about actual data brokers.

Writing in support, Californians for Consumer Privacy state:

> Unfortunately, recent reporting has documented how location data is being harvested from apps on phones, sold to data brokers who aggregate that data with other personal data, and then offer third parties the ability to precisely track a consumer's movements. Recent headlines highlighting this include an LGBTQ dating app and a Muslim prayer app selling data on people's location to a data broker, and data brokers advertising the sale of real-time location data of active military personnel. This chilling violation of privacy highlights that much of our sensitive personal data is used by data brokers to profile us.
>
> To better protect against the potential misuse of personal data, Californians need more rights and better visibility regarding data brokers. SB 1059 will help achieve this by strengthening key aspects of the state's existing data broker laws, as well as empowering the California Privacy Protection Agency (PPA) — the agency that was created with the passage of the CPRA — to regulate data brokers. [footnotes omitted]

5. <u>Furthering the purpose and intent of the CPRA</u>

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

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.

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 furthers the purposes and intent of the CPRA.

SUPPORT

5Rights Foundation
ACLU California Action
Californians for Consumer Privacy
Consumer Reports
Consumer Watchdog
Electronic Frontier Foundation
Electronic Privacy Information Center
Privacy Rights Clearinghouse

OPPOSITION

Association of National Advertisers
California Chamber of Commerce
California Grocers Association
California Retailers Association
Insights Association
Internet Coalition
Technet

RELATED LEGISLATION

Pending Legislation:

SB 746 (Skinner, 2022) amends the CCPA to require businesses to disclose whether they use the personal information of consumers for political purposes, as defined, to consumers, upon request, and annually to the Attorney General or the PPA, as specified. This bill is currently awaiting referral in the Assembly.

SB 1454 (Archuleta, 2022) removes the sunset on the exemption from certain provisions of the CCPA of personal information reflecting a communication or a transaction between a business and a company, partnership, sole proprietorship, nonprofit, or government agency that occurs solely within the context of the business conducting due diligence or providing or receiving a product or service. It also makes permanent the exemption for personal information that is collected and used by a business solely within the context of having an emergency contact on file, administering specified benefits, or a person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business. This bill is currently in this Committee.

AB 2871 (Low, 2022) is identical to SB 1454. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

AB 2891 (Low, 2022) is substantially similar to SB 1454 and AB 2871, but extends, rather than removes, the sunset to January 1, 2026. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

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.

****