Date of Hearing: June 27, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
SB 362 (Becker) – As Amended May 18, 2023

As Proposed to be Amended

SENATE VOTE: 32-8

SUBJECT: Data brokers: privacy

SYNOPSIS

Data brokers are businesses that purchase information about us from multiple sources, combine this information to build comprehensive datasets about us and our lives, and offer this information for sale to anyone able to pay for it.

In 2019, the Legislature enacted AB 1202 (Chau, Chap. 753, Stats. 2019), the Data Broker Registration Law, which requires entities that meet the bill's definition of "data broker" to register with the California Attorney General. The Attorney General, in turn, posts this information to a public website. The website now lists approximately 500 registered data brokers.

Data brokers offer many benefits to consumers, including financial fraud detection and prevention, facilitating loan and insurance approvals, and making it easier to find people one has lost touch with. Nevertheless, there have been myriad reports of the risks data brokers pose to individuals' Constitutional rights, financial privacy, personal privacy, and reproductive privacy. The risks for undocumented individuals are particularly heightened.

In response to these risks, this bill proposes to strengthen the Data Broker Registration Law. The most important change would require the California Privacy Protection Agency to establish an "accessible deletion mechanism," Beginning on July 1, 2026, the mechanism would allow a consumer to make a single secure and verifiable request that data brokers which maintain personal information about the consumer proceed to delete that information—and to continue to delete personal information received about them in perpetuity. Data brokers would have to consult the accessible deletion mechanism at least every 31 days and process all outstanding deletion requests.

This analysis addresses the following questions:

1) *What is a data broker?*
2) *What benefits do data brokers offer?*
3) *What risks do data brokers pose?*
4) *What California laws regulate data brokers?*
5) *In what ways are California laws regulating data brokers arguably ineffective at protecting consumer privacy?*
6) *What would this bill do?*
7) *What trade-offs does this bill pose?*

Committee amendments are set forth and summarized at the end of the analysis. One significant amendment removes the Attorney General from administering and enforcing the Data Broker Registration Law, instead placing sole authority with the Privacy Agency. Another significant amendment would allow consumers to selectively exclude specific data brokers from a deletion request, and to revoke previously-made deletion requests, thereby ensuring that deletion requests are not irrevocable.

This bill is sponsored by Privacy Rights Clearinghouse, and supported by more than two dozen nonprofit organizations, including Planned Parenthood Affiliates of California and a number of legal aid organizations. It is opposed by two coalitions, one a group of trade associations representing the advertising industry, and another a broader group of trade associations that includes the California Chamber of Commerce and TechNet.

If passed by this Committee, the bill will next be heard by the Assembly Judiciary Committee.

SUMMARY: Strengthens the Data Broker Registration Law, including by requiring the California Privacy Protection Agency to introduce, by July 1, 2026, an accessible deletion mechanism whereby consumers can request registered data brokers to delete their personal information in perpetuity. Specifically, **this bill**:

1) Clarifies that, unless otherwise specified, definitions of terms defined under the California Consumer Privacy Act (CCPA) also apply when used under the Data Broker Registration Law (DBRL).

2) Alters existing provisions of the DBRL as follows:

    a) Extends exclusions from the definition of "data broker" to encompass all entities covered by the federal Fair Credit Reporting Act and the federal Gramm-Leach-Bliley Act, rather than just consumer reporting agencies and financial institutions, respectively.

    b) Provides that the registration fee to be collected from data brokers must also cover the reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described below.

    c) Requires deposit of all registration fees and all penalties, fees, and expenses recovered from enforcement in the Data Brokers' Registration Fund.

    d) Provides for the Data Brokers' Registration Fund to be administered by the California Consumer Privacy Agency (Privacy Agency), and that these funds are to be available for the following purposes, in addition to the existing purpose of maintaining an informational website:

        i) The costs incurred by the state courts and the Privacy Agency in enforcing the DBRL.

        ii) The reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described below.

    e) Requires data brokers to register with the Privacy Agency, rather than the Attorney General.

f) Requires the Privacy Agency, rather than the Attorney General, to create the internet website where data broker registration information is made available.

g) Increases civil penalties for non-registration from one hundred dollars ($100) to two hundred dollars ($200) per day.

h) To the extent not described above, removes statutory authority from the Attorney General and the California Department of Justice to administer and enforce the DBRL, instead placing this authority with the Privacy Agency.

3) Adds the following to the information to be collected from data brokers as part of the annual registration process:

a) The information called for in 4) a) and b) below.

b) Whether the data broker collects the personal information of minors.

c) Whether the data broker collects consumers' precise geolocation.

d) Whether the data broker collects consumers' reproductive health care data.

e) Beginning January 1, 2029, whether the data broker has undergone the audit required under this bill, and if so, the most recent year that the data broker submitted an audit report and any related materials to the Privacy Agency.

f) A link to a page on the data broker's internet website that details how consumers may exercise the following privacy rights under the CCPA, without using dark patterns:

i) Delete personal information.

ii) Correct inaccurate personal information.

iii) Learn what personal information is being collected and how to access that personal information.

iv) Learn what personal information is being sold or shared and to whom.

v) Learn how to opt out of the sale or sharing of personal information.

vi) Learn how to opt out of the sale or sharing of sensitive personal information.

g) Whether and to what extent the data broker or any of its subsidiaries is regulated by the federal Fair Credit Reporting Act, the federal Gramm-Leach-Bliley Act, or the California Insurance Information and Privacy Protection Act.

4) Requires that, on or before January 31 following each year in which a business meets the definition of "data broker," that it:

a) Compile the number of requests it received to exercise the CCPA rights set forth under 3) f) above.

b) Compile the median and mean number of days within which the data broker substantively responded to the categories of requests listed in a).

c) Compile the number of requests that the data broker denied in whole or in part because of any of the following:

i) The request was unverifiable.

ii) The request was not made by a consumer.

iii) The request called for information exempt from disclosure.

iv) The request was denied on other grounds.

d) Disclose the data in a), b), and c) on its website and provide a link to that website in its privacy policy.

5) Requires, by January 1, 2026, the Privacy Agency to establish an accessible deletion mechanism that does all of the following:

a) Allows a consumer, through a single verifiable request, to request that every data broker that maintains personal information related to that consumer, whether held by the data broker or an associated service provider or contractor, delete that information.

b) Implements and maintains reasonable security procedures and practices, including, but not limited to, administrative, physical, and technical safeguards i) appropriate to the nature of the information and the purposes for which the personal information will be used and ii) to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

c) Allows a consumer to selectively exclude specific data brokers from a deletion request under this paragraph 5).

d) Allows a consumer to make a request to undo or alter a previous request made under this paragraph 5), provided that at least 31 days have passed since the consumer last made a request.

6) Provides that the accessible deletion mechanism must meet all of the following requirements:

a) Allow a consumer to request the deletion of all personal information related to that consumer through a single deletion request.

b) Permit a consumer to securely submit information in one or more privacy-protecting ways determined by the Privacy Agency to aid in the deletion request.

c) Allow data brokers registered with the Privacy Agency to determine whether an individual has submitted a verifiable deletion request, without allowing the disclosure of any additional personal information (except as otherwise specified in the DBRL).

d) Not charge a consumer to make a deletion request.

e) Allow a consumer to make a deletion request in any language spoken by any consumer for whom personal information has been collected by data brokers.

f) Be readily accessible and usable by consumers with disabilities.

g) Support the ability of a consumer's authorized agent to aid in the deletion request, as specified in applicable regulations under the California Consumer Privacy Act.

h) Allow the consumer, or their authorized agent, to verify the status of the deletion request.

7) Requires, beginning August 1, 2026, a data broker to access the deletion mechanism at least once every 31 days and do all of the following:

a) Process all deletion requests, and delete all personal information related to the consumers making the requests.

b) Direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the consumers making the requests.

c) Send an affirmative representation to the Privacy Agency indicating the number of records deleted by the data broker and any service providers or contractors directed to delete personal information.

8) Clarifies that a data broker is not required to delete a consumer's personal information if maintaining the information is reasonably necessary to fulfill one of the purposes that the CCPA also exempts from deletion requests, e.g., complying with the California Electronic Communications Privacy Act.

9) Further clarifies that the exemption under 8) permits a data broker to only fulfill the purpose in question, and may not be used for any other purpose, including, but not limited to, marketing purposes.

10) Permits the Privacy Agency to charge an access fee to a data broker when the broker accesses the deletion mechanism. The fee may not exceed the reasonable costs of providing that access. The fee is to be deposited in the Data Brokers' Registry Fund.

11) Requires, beginning July 1, 2026, that if a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this bill, the data broker shall thereafter delete all personal information of the consumer at least once every 31 days unless the consumer requests otherwise.

12) Requires data brokers to comply with the following compliance requirements:

a) Beginning January 1, 2028, and every three years thereafter, undergo an audit by an independent third party to determine compliance with this bill.

b) Submit a report resulting from the audit, and any related materials, to the Privacy Agency within five business days of the Agency's written request.

c) Maintain this report and the related materials for at least six years.

13) Provides for administrative enforcement by the Privacy Agency of specified DBRL requirements.

14) Establishes a five year statute of limitations for the Privacy Agency to bring an administrative action under the DBRL.

15) Grants the Privacy Agency authority to adopt regulations, pursuant to the Administrative Procedure Act, to implement and administer the DBRL, except that that regulations establishing fees are exempt from the Act.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Establishes the Data Broker Registration Law (DBRL). (Civ. Code §§ 1798.99.80-1798.99.88.)

3) 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. (Civ. Code § 1798.99.80(d).)

4) Excludes from the definition of "data broker" all of 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.

   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(d)(1)-(3).)

5) Requires the Attorney General to create a page on its internet website where information provided from data brokers is made accessible to the public. (Civ. Code § 1798.99.84.)

6) Creates the Data Brokers' Registry Fund within the State Treasury, to offset costs of establishing and maintaining the informational website under 3). (Civ. Code § 1798.99.81.)

7) Requires that, on or before January 31 following each year in which a business meets the definition of "data broker," that it register with the Attorney General. (Civ. Code § 1798.99.82(a).)

8) Sets forth the following steps for a data broker to follow to register with the Attorney General:

   a) Pay a registration fee, in an amount determined by the Attorney General, not to exceed the reasonable costs of establishing and maintaining the informational website under 3). Registration fees are deposited in the Data Brokers' Registry Fund. (Civ. Code § 1798.99.82(b)(1).)

b) Provide its name; primary physical, email, and internet website addresses; and any additional information or explanation it chooses to provide concerning its data collection practices. (Civ. Code § 1798.99.82(b)(2).)

9) Makes a data broker that fails to register subject to an injunction and liable for civil penalties, fees, and costs in an action brought by the Attorney General, as follows:

   a) Civil penalties are one hundred dollars ($100) per day for each day the data broker failed to register.

   b) Fees that were due during the period the data broker failed to register.

   c) Expenses incurred by the Attorney General in investigating and prosecuting the action. (Civ. Code § 1798.99.82(c).)

10) 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.)

11) Provides that the provisions set forth above do not supersede or interfere with the operation of the California Consumer Privacy Act. (Civ. Code § 1798.99.88.)

12) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

13) Defines the following terms under the CCPA:

   a) "Business" means a for-profit entity that collects consumers' personal information, does business in California, and meets one or more of the following criteria:

      i) It had gross annual revenue of over $25 million in the previous calendar year.

      ii) It buys, receives, or sells the personal information of 100,000 or more California residents, households, or devices annually.

      iii) It derives 50% or more of its annual revenue from selling California residents' personal information. (Civ. Code § 1798.140(d).)

   b) "Collects" and "collection" mean buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. The term includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior. (Civ. Code § 1798.140(f).)

   c) "Consumer" means a natural person who is a California resident. (Civ. Code § 1798.140(i).)

   d) "Personal information" means 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. Personal information includes such information as:

i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

iii) Biometric information.

iv) Internet activity information, including browsing history and search history.

v) Geolocation data.

vi) Professional or employment-related information. (Civ. Code § 1798.140(v).)

e) "Sell" means, with certain exceptions, selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration. (Civ. Code § 1798.140(ad).)

f) "Third party" means a person who is not any of the following:

i) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under the CCPA.

ii) A service provider to the business.

iii) A contractor. (Civ. Code § 1798.140(ai).)

14) Establishes the Privacy Agency, vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

15) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.120.)

e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

16) Enumerates exemptions under which a business is not required to comply with a consumer's request to delete personal information, for cases in which it is reasonably necessary to maintain this information, such as for debugging errors and to comply with the California Electronic Communications Privacy Act (CalECPA). (Civ. Code § 1798.105(d).)

17) Specifies procedures whereby the Privacy Agency may bring administrative enforcement actions to address CCPA violations. (Civ. Code §§ 1798.199.45, 1798.199.50, 1798.199.55, 1798.199.60.)

18) Establishes administrative penalties for CCPA violations, to be recovered through administrative enforcement actions brought by the Privacy Agency. (Civ. Code § 1798.155.)

19) Provides five years from the date upon which a violation of the CCPA occurred for the Privacy Agency to bring an administrative enforcement action. (Civ. Code § 1798.199.70.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS:

1) **Background.** At this point, most people know that when they use a "free" service on the Internet (one for which there is no monetary charge), they are actually paying for it in the form of the data they reveal about themselves: the contents of their messages, their reactions to social media posts, their GPS coordinates when they use their phones, the identities of their contacts, and so on. Most also realize that many of the paid products and services they use also reveal data about them, whether it's their smart speaker, their online newspaper, or their favorite streaming service. And just about everyone knows that, once collected, the data they have revealed is used to serve targeted advertising back to them. A person who belongs to Facebook groups for Corvette owners and watches Corvette documentaries online is going to see online ads related to Corvettes. None of this is surprising, and for most of us, it is a slightly-uncomfortable quid pro quo that we pay for the convenience and pleasure of using networked technology.

But there is a much broader group of companies, known as *data brokers*, that purchase information about us from multiple sources, combine it to build comprehensive datasets about us and our lives, and offer this information for sale to anyone who might be able to pay for it. As summarized in a report issued by Duke University's public policy program: "[D]ata brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel,

and on current U.S. government employees." (Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke University Sanford Cyber Policy Program (Aug. 2021), *available at* https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.) Their brokering of our data is basically unregulated. "Virtually nothing in current U.S. law limits their selling that data to a range of actors, from insurance firms to U.S. law enforcement agencies to foreign entities." (*Id.* at p. 2.) Increasing awareness, and concern, at the highest levels of government: "Unchecked social media data collection has been used to threaten people's opportunities, undermine their privacy, or pervasively track their activity—often without their knowledge or consent." https://www.whitehouse.gov/ostp/ai-bill-of-rights/

In 2019, the Legislature enacted AB 1202 (Chau, Chap. 753, Stats. 2019), the Data Broker Registration Law, which required entities that meet the bill's definition of "data broker" to register with the California Attorney General and disclose their name; primary physical, email, and internet website addresses; and any additional information they choose to provide regarding their data collection practices. The Attorney General, in turn, posts this information to a public website, available at https://www.oag.ca.gov/data-brokers. The website now lists approximately 500 registered data brokers.

2) **Author's statement.** 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. […] By enhancing transparency and giving consumers more control over their data, SB 362 represents an important step forward in protecting our privacy rights.

3) **What is a data broker?** The Federal Trade Commission (FTC) defines data brokers as "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud." (FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014) p. 3, *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.)

The Data Broker Registration Law 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." (Civ. Code § 1798.99.80(d).)

The common point in both of these definitions is that there is no direct relationship between a consumer and any data broker that has information about the consumer. In fact, it is unclear whether "consumer" is even an apt term in this context, since the person whose data is being collected generally does not directly consume any products or services produced by the data broker. Nevertheless, since "consumer" has become the default term in this context, it will be used in this analysis.

The key point to understand is that no consumer chooses to have a relationship with a data broker. There is certainly a consensual transaction between the consumer and the websites the consumer accesses; the apps the consumer uses; and the consumer's cell phone and internet service providers. Each of these transactions involves a transfer of the consumer's personal information to these entities. But the consumer is not involved in the subsequent sale or transfer of their personal information to data brokers; there is no transaction between the consumer and the data broker involved with that sale or transfer.

4) **What benefits do data brokers offer?** At the outset, it is important to realize that the majority of the information and services that data brokers sell is intended for legitimate purposes. As noted in an opposition letter from four advertising trade groups (American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, and Digital Advertising Alliance):

> Data brokers are vital to new and small businesses' ability to thrive and find new customers. Much like supply chain partners create value in various sectors of the economy, data brokers serve as intermediaries that engage in specialized techniques and practices to help their clients find and attract new and existing customers. Data brokers enable small businesses to leverage more than just the data they receive from direct interactions with their niche customer base. […] Information obtained from data brokers makes it possible for small and mid-size companies with less resources to spend on advertising to reach as many new potential customers as possible and in the most efficient and accountable ways possible. In large part due to services provided by data brokers, small and mid-sized businesses are empowered to compete with larger companies who have more resources to allocate to broad marketing efforts.

Another opposition group, consisting of a number of trade associations, including California Chamber of Commerce and TechNet, writes:

> Data brokers provide services to many other businesses in support of legitimate purposes that protect or benefit consumers, including anti-money laundering, cybersecurity, and underwriting activities. They are widely used by an array of public and private entities and individuals. For example, law enforcement agencies may use the services to serve subpoenas or to identify and locate witnesses and suspects. Welfare agencies can use the services to find parents evading child support awards. Businesses use the services to detect order fraud and update customer databases.

Coresignal, a data broker registered in California under the name Deeptrace, identifies four major categories of services provided by data brokers:

> *Marketing and sales.* Among the most commonly recognized data brokers are those that provide information for the purpose of targeted marketing…. Such providers create databases with information such as a professional's age, income, buying habits, internet activity, and

> similar, helping to create their consumer profile. For certain companies, this information might become a sales lead that they could then target through specific marketing strategies.
>
> *Fraud detection*. Some data brokers specialize in double-checking the information on people or businesses in order to prevent possible fraud. For example, banks or financial firms might turn to a data broker to find out more about an entity before granting a loan. The data that the broker holds or can collect might help establish the accuracy of the information provided by the loan [applicant], thus preventing granting a fraudulent claim.
>
> *Risk mitigation.* Banks and loan firms also use data brokers to calibrate the loan offers for particular applicants. Such a data broker would then collect financial data and information such as online purchase history, from which companies could determine the individual's financial situation and predict buying intent. This would let the bank know what size of loan could be risked with that person and the interest rate that should be set. Information brokers are also used for the purposes of risk mitigation by insurance companies, as particular website visits or purchases of medical items might indicate higher medical risks, thus making the insurer raise the interest rates of health insurance.
>
> *People search*. A data broker of this type would create a database about private people that may be accessed through the broker's website. The website might provide general biographic data such as date of birth, education and employment history, marital status, and such personal information as affiliations and interests. Professional profile websites, also known as people search websites, are used by private individuals to retrace lost contacts or simply find out more about acquaintances. Companies use these websites for various…purposes, such as job candidate ranking[.] (Coresignal, *What is a Data Broker and Why Do You Need One?* (Sep. 16, 2022), *available at* https://coresignal.com/blog/data-broker/.)

5) **What risks do data brokers pose?** The risks posed by data brokers are longstanding and well-documented.

Risks to Constitutional rights. In *Carpenter v. United States* (2018) 585 U.S. __, 138 S. Ct. 2206, the U.S. Supreme Court held that because "individuals have a reasonable expectation of privacy in the whole of their physical movements" under the Fourth Amendment, law enforcement and other governmental entities must obtain a search warrant to obtain a person's cell phone location history from their wireless provider. Nevertheless, as reported by *The Wall Street Journal*:

> The federal government has essentially found a workaround by purchasing location data used by marketing firms rather than going to court on a case-by-case basis. Because location data is available through numerous commercial ad exchanges, government lawyers have approved the programs and concluded that the *Carpenter* ruling doesn't apply. (Tau, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, The Wall Street Journal (Feb. 7, 2020), *available at* https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.)

California law enforcement agencies could potentially use the same workaround to avoid the nuanced requirements of the California Electronic Communications Privacy Act, which generally prohibits law enforcement from accessing electronic communication information without a warrant or other court process.

Risks to financial privacy. Information collected and sold by data brokers can lead to financial fraud. In 2014, the Federal Trade Commission sued LeapLab, a data broker that purchased payday loan applications from websites, called "publishers," which help consumers apply for payday loans. Key paragraphs from the FTC's court complaint are as follows:

> 13. Defendants collected hundreds of thousands of consumer payday loan applications from thousands of payday loan websites [...]
>
> 15. Most applications collected by Defendants contained the consumer's name, address, phone number, employer, Social Security number, and bank account number, including the bank routing number. […]
>
> 18. Defendants sold approximately five (5) percent of these applications to online lenders, which paid Defendants between approximately $10 and $150 per lead.
>
> 19. Defendants monetized the remaining 95 percent by selling these applications for approximately $0.50 each to non-lender third parties that did not use the information to assist consumers in obtaining a payday loan or other extension of credit. [...]
>
> 25. Between 2009 and 2013, Ideal Financial purchased at least 2.2 million consumers' financial information from data brokers and used it to make millions of dollars in unauthorized debits and charges. […]
>
> 28. LeapLab provided Ideal Financial with financial account information for at least 16 percent of Ideal Financial's victims. (Complaint, *FTC v. Sitesearch Corp dba LeapLab* (D. Ariz.) No. CV-14-02750-PHX-NVW, *available at* https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf.)

Even if one is more financially secure than the typical payday loan applicant, data brokers collect sufficient personal information about many individuals to facilitate identity theft. And this is to say nothing of the risks from this information being released through a data breach. According to one information security professional who investigated data security on data broker websites several years ago:

> Firstly, data broker protective measures are woeful... Secondly, it means we are now entering the age of the mega breach. In the way that breaches in the hundreds of millions of records are becoming the norm today, we will soon become accustomed to breaches containing billions of records a few years from now. Lastly, this is an area crying out for regulation. Opening up access to larger and larger pools of consumer data should bring with it corresponding shifts in security obligations, which are sadly lacking today—at least in the United States. Until then, it's watch and wait. (Haynes, *Are Data Brokers Actually Secure?*, InfoSecurity Magazine (Aug. 15, 2017), *available at* https://www.infosecurity-magazine.com/opinions/are-data-brokers-actually-secure/.)

Risks to personal privacy. Information collected and sold by data brokers can reveal the entirety of an individual's movements, as revealed by their cellphone's location. The Federal Trade Commission recently sued Kochava, a data broker registered with California. According to the FTC:

> Kochava acquires location data from other data brokers based on information collected from consumers' mobile devices. Kochava then compiles it in customized data feeds, which it markets to commercial clients eager to know where consumers are and what they're doing. The amount of location data Kochava has about consumers is staggering. In pitching its products, Kochava offers what it describes as "rich geo data spanning billions of devices globally," further claiming that its location feed "delivers raw latitude/longitude data with volumes around 94B+ geo transactions per month, 125 million monthly active users, and 35 million daily active users, on average observing more than 90 daily transactions per device." […] Kochava sold access to its data feeds on publicly accessible information marketplaces and, until just recently, even made free samples available with what the FTC describes as "only minimal steps and no restrictions on usage." […T]o gain access to a sample, a potential customer could use an ordinary personal email address and describe their intended use with something as generic as "business." (Fair, *FTC says data broker sold consumers' precise geolocation, including presence at sensitive healthcare facilities*, Federal Trade Commission Business Blog (Aug. 29, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare.)

Key paragraphs from the FTC's court complaint against Kochava are as follows:

> 24. [T]he data sold by Kochava may be used to identify individual consumers and their visits to sensitive locations. The sale of such data poses an unwarranted intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers.
>
> 25. For example, the data may be used to identify consumers who have visited an abortion clinic and, as a result, may have had or contemplated having an abortion. In fact, in just the data Kochava made available in the Kochava Data Sample, it is possible to identify a mobile device that visited a women's reproductive health clinic and trace that mobile device to a single-family residence. The data set also reveals that the same mobile device was at a particular location at least three evenings in the same week, suggesting the mobile device user's routine. The data may also be used to identify medical professionals who perform, or assist in the performance, of abortion services.
>
> 26. As another example, the data could be used to track consumers to places of worship, and thus reveal the religious beliefs and practices of consumers. In fact, the Kochava Data Sample identifies mobile devices that were located at Jewish, Christian, Islamic, and other religious denominations' places of worship.
>
> 27. As another example, the data could be used to track consumers who visited a homeless shelter, domestic violence shelter, or other facilities directed to at-risk populations. This information could reveal the location of consumers who are escaping domestic violence or other crimes. (Complaint, *FTC v. Kochava Inc.* (D. Idaho) No. 2:22-cv-00377-DCN, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.)

Risks to reproductive privacy. Last year, *Motherboard*, a tech-focused news site operated by *Vice*, released the results of its investigation into SafeGraph, a data broker registered with California:

> A location data firm is selling information related to visits to clinics that provide abortions including Planned Parenthood facilities, showing where groups of people visiting the locations came from, how long they stayed there, and where they then went afterwards, according to sets of the data purchased by *Motherboard*. […] The sale of the location data raises questions around why companies are selling data based on abortion clinics specifically, and whether they should introduce more safeguards around the purchase of that information, if [they should be] be selling it at all. […]
>
> SafeGraph classifies "Planned Parenthood" as a "brand" that can be tracked, and the data Motherboard purchased includes more than 600 Planned Parenthood locations in the United States. The data included a week's worth of location data for those locations in mid-April. SafeGraph calls the location data product "Patterns." In total, the data cost just over $160. Not all Planned Parenthood locations offer abortion services. But *Motherboard* verified that some facilities included in the purchased dataset do. […]
>
> SafeGraph calculates where it believes visitors to a location live to the census block level. SafeGraph does this by analyzing where a phone is commonly located overnight, the company's documentation suggests. (Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Motherboard (May 3, 2022), *available at* https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.)

This story was published before the U.S. Supreme Court released its opinion in *Dobbs v. Jackson Women's Health Org.* (2022) 597 U.S. __ (repealing the constitutional right to an abortion). After the story was published, SafeGraph agreed to remove this data from its product. (Kaye, *SafeGraph is under fire for selling abortion data*, Protocol (May 4, 2022), *available at* https://www.protocol.com/enterprise/safegraph-auren-hoffman-abortion-data.) But there is no way of knowing whether any of hundreds of other data brokers might be collecting and selling similar information.

Particularly given the significant efforts the Legislature has made to protect the privacy of those coming to California in search of safe and legal abortions, other forms of reproductive health care, and gender-affirming health care, it is troubling that a person might nevertheless find themselves criminally prosecuted based on information available from data brokers.

Risks to undocumented immigrants. The ability to purchase data about a person from data brokers poses special risks to undocumented individuals. A recent article addresses ICE's contract with LexisNexis, a data broker registered with California:

> LexisNexis is known for its vast trove of public records and commercial data, a constantly updating archive that includes information ranging from boating licenses and DMV filings to voter registrations and cellphone subscriber rolls. In the aggregate, these data points create a vivid mosaic of a person's entire life, interests, professional activities, criminal run-ins no matter how minor, and far more. […] LexisNexis has turned the mammoth pool of personal data into a lucrative revenue stream by selling it to law enforcement clients like ICE, who use the company's many data points on over 280 million different people to … locate and apprehend them. […] LexisNexis is empowering ICE to sift through a large sea of personal data to do exactly what advocates have warned against: busting migrants for civil immigration violations, a far cry from thwarting terrorists and transnational drug cartels. (Biddle, *LexisNexis is selling your personal data to ICE so it can try to predict crimes*, The

Intercept (Jun. 20, 2023), *available at* https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/.)

Again, given the extraordinary efforts the Legislature has made to protect undocumented Californians from ICE abuses, it is alarming that these protections can be circumvented through using a data broker.

6) **What California laws regulate data brokers?** Data brokers are currently regulated by two principal laws in California: the Data Broker Registration Law (DBRL), Civ. Code §§ 1798.99.80-1798.99.88, and the California Consumer Privacy Act (CCPA), Civ. Code §§ 1798.100-1798.199.100.

The DBRL is comprehensively summarized in paragraphs 2) – 11) under **EXISTING LAW** above. The DBRL's key provision requires any business that meets the definition of "data broker" to register with the Attorney General annually by paying a registration fee and providing its name; primary physical, email, and internet website addresses; and any additional information or explanation it chooses to provide concerning its data collection practices. (Civ. Code § 1798.99.82.) The Attorney General, in turn, must establish a page on its internet website making this information accessible to the public. (Civ. Code § 1798.99.84.)

Relevant provisions of the CCPA are summarized in paragraphs 12) – 19) under **EXISTING LAW** above. Data brokers are subject to the CCPA because they collect consumers' personal information, do business in California, and more than likely meet one or more of the following criteria: (i) having gross annual revenue of over $25 million in the previous year; (ii) buying, receiving, or selling the personal information of 100,000 or more California residents, households, or devices annually; or (iii) derives 50% or more of their annual revenue from selling California residents' personal information. (Civ. Code § 1798.140(d).)

7) **In what ways are California laws regulating data brokers arguably ineffective at protecting consumer privacy?** There are several reasons why current California laws cannot effectively protect consumers who do not wish their personal information to be held or used by data brokers:

1. According to information provided by the author's office, as of May 29, 2023, 496 data brokers were registered with the state of California and therefore listed on the AG's registry website at https://www.oag.ca.gov/data-brokers.

2. The CCPA allows businesses to provide consumers various methods to exercise their CCPA rights. Different data brokers use different methods, including referring consumers to a page on the data broker's own website; referring consumers to third-party CCPA management services; providing a toll-free number to call; providing an email address to email; providing a mailing address to write to; and providing a webform for consumers to fill out.

3. Deletion requests under the CCPA only cover the personal information that the business has collected about the consumer at the time the consumer makes the deletion request. So when new personal information about the consumer reaches a data broker post-deletion request, the data broker can begin using and selling that information just as before.

Few people have the time to access 496 websites, identify each site's particular deletion mechanism, and use that mechanism to request deletion of their personal information. And no one has the time to repeat that process over and over, for the rest of their lives.

But there is an even more fundamental problem. The right of deletion under the CCPA provides: "A consumer shall have 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) [emphasis added].) A data broker by statutory definition "does not have a direct relationship" with consumers. (Civ. Code § 1798.99.80(d).) It buys information about consumers from others. So it will not have collected information from the consumer. Therefore, a deletion request directed at a data broker will likely be ineffective at deleting information about the consumer that is in the data broker's possession.

The bill's opponents dispute this point, arguing that the CCPA's right of deletion also provides as follows:

> A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information … shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, **and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information** unless this proves impossible or involves disproportionate effort. (Civ. Code §105(c) [emphasis added].)

According to these opponents, "Thus, data brokers are subject to CCPA deletion requests if they buy or receive PI from another business."

There are at least two flaws with this line of argument. First, in order to ensure data broker deletion of their personal information, a person would have to direct a deletion request to every business that has ever collected personal information about them. Compiling such a list is likely an impossible task. Second, as discussed above under #3, deletion requests are only effective at the point in time they are made; once new personal information about the consumer reaches a data broker, it can resume using and selling information about the consumer.

In sum, it hardly matters that one has deletion rights if, as a practical matter, no one can exercise them where data brokers are concerned. But deletion is a must if one is concerned with protecting oneself from the risks set forth above. Even if one were to instead, say, exercise the CCPA right to opt-out of sale or sharing of personal information by a data broker, one would still have to (i) exercise that right 496 times and (ii) continually monitor the data broker registry for new data brokers with which to submit "opt-out" requests. This would be a difficult task for most people, and likely impossible for those who urgently need to safeguard their privacy, such as domestic violence victims. It would also require faith that no data broker holding one's information were ever the victim of a data breach.

8) **What would this bill do?** In response to the foregoing deficiencies in data broker privacy, this bill would amend the DBRL to do the following:

1. As proposed to be amended, transfer responsibility for administering the DBRL from the Attorney General to the Privacy Agency.

2. Require the Privacy Agency to establish an "accessible deletion mechanism." Beginning on July 1, 2026, it would allow a consumer to make a single secure and verifiable request that every data broker which maintains personal information about the consumer proceed to delete that information—and to continue to delete personal information received about them in perpetuity. Beginning August 1, 2026, data brokers would have to consult the accessible deletion mechanism at least every 31 days and process all outstanding requests.

   The accessible deletion mechanism is the heart of the bill: it is intended to solve the myriad problems and loopholes set forth above, and finally make it practicable for a person to ensure that data brokers actually delete their personal information.

3. As proposed to be amended, allow consumers to selectively exclude data brokers of their choice from the accessible deletion mechanism, and also allow consumers to revoke previously-made deletion requests. In other words, deletion requests could be tailored to consumers' needs and would not be irrevocable.

4. Augment the information collected from data brokers as part of the annual registration process to include, among other things, a link to a page on the data broker's website where consumers can exercise their CCPA rights, and data regarding the number of CCPA requests the data broker received in the previous year.

5. Require data brokers, beginning January 1, 2028, to obtain an audit once every three years regarding their compliance with this bill, and to make the audit report and related materials available to the Privacy Agency upon written request.

6. Increase civil penalties for non-registration from $100 per day to $200 per day.

7. Provide for administrative enforcement of the bill's requirements by the Privacy Agency, including a five-year statute of limitations that matches the limitations period under the CCPA.

9) **What trade-offs does this bill pose?** If this bill is enacted, the myriad of risks presented by data brokers holding one's personal information will likely induce many consumers to request deletion of their data.

That said, as discussed above, data brokers provide useful services for many people. When a consumer uses a credit card while traveling, the bank likely consults a data broker to verify that the consumer is actually in that location, thus eliminating the cumbersome process of declining the transaction and requiring the consumer to call and verify their presence. Many transactions, such as obtaining a loan or an insurance quote, likely proceed faster because much of the relevant underwriting data can be obtained from a data broker rather than having to be assembled by hand. As the bill's opponents from the advertising industry note, small businesses benefit greatly from being able to target their products and services to customers who are likely to want them, thereby saving precious resources.

Ideally, one would be able to retain the benefits offered by worthwhile data broker services while minimizing the overall risks to one's privacy and safety. Proposed amendments to the bill, set forth below, are intended to facilitate this goal. They would allow a consumer to selectively exclude data brokers from a deletion request. The amendments would also allow a consumer,

once at least 31 days have passed, to amend or revoke a previous deletion request. So, if one finds, after making a deletion request, that one or more data brokers provides valuable services that one needs, one can request that data broker to once again collect and retain one's personal information.

These amendments should increase the importance of an existing feature of the DBRL: when registering, a data broker is free to submit "[a]ny additional information or explanation the data broker chooses to provide concerning its data collection practices," and have this information reflected in the data broker registry. (Civ. Code §§ 1799.99.82 (b)(2)(B), 1799.99.84.) It is hoped that data brokers that want to be excluded from deletion requests would be incentivized, under this bill, to provide accurate information about the ways in which they benefit consumers, and be disincentivized from engaging in privacy-violating practices.

10) **Committee amendments**. All of the proposed amendments set forth below are to provisions of the Civil Code.

The following amendments have the effect of removing the Attorney General and the California Department of Justice from administering and enforcing the DBRL, instead placing sole authority with the Privacy Agency.

1798.99.81. A fund to be known as the "Data Brokers' Registry Fund" is hereby created within the State Treasury. ***The fund shall be administered by the California Privacy Protection Agency.*** ~~All registration fees received pursuant to paragraph (1) of subdivision (b) of Section 1798.99.82 and all penalties, fines, fees, and expenses received in an action prosecuted under subdivisions (c) to (f), inclusive, of Section 1798.99.82.~~ ***All moneys collected or received by the California Privacy Protection Agency and the Department of Justice under this title*** shall be deposited into the Data Brokers' Registry Fund, to be available for expenditure by ~~the Department of Justice and the~~ California Privacy Protection Agency, upon appropriation by the Legislature, to offset all of the following costs:

(a) The reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84.

(b) The costs incurred by the state courts~~,~~ ***and*** the California Privacy Protection Agency~~, and the Attorney General~~ in connection with enforcing this title, as specified in Section 1798.99.82.

(c) The reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in Section 1798.99.86.

1798.99.82. (a) On or before January 31 following each year in which a business meets the definition of data broker as provided in this title, the business shall register with the California Privacy Protection Agency pursuant to the requirements of this section.

[…]

~~(c) A data broker that fails to register as required by this section is subject to injunction and is liable for civil penalties, fees, and costs in an action brought in the name of the people of the State of California by the Attorney General as follows:~~

~~(1) A civil penalty of two hundred dollars ($200) for each day the data broker fails to register as required by this section.~~

~~(2) An amount equal to the fees that were due during the period it failed to register.~~

~~(3) Expenses incurred by the Attorney General in the investigation and prosecution of the action as the court deems appropriate.~~

~~(d)~~ ***(c)*** A data broker that fails to register as required by this section is liable for administrative fines and costs in an administrative action brought by the California Privacy Protection Agency as follows:

(1) An administrative fine of two hundred dollars ($200) for each day the data broker fails to register as required by this section.

(2) An amount equal to the fees that were due during the period it failed to register.

(3) Expenses incurred by the California Privacy Protection Agency in the investigation and administration of the action as the court deems appropriate.

~~(e) A data broker required to register under this title that fails to comply with the requirements of Section 1798.99.86 is subject to injunction and is liable for civil penalties, fees, and costs in an action brought in the name of the people of the State of California by the Attorney General as follows:~~

~~(1) A civil penalty of two hundred dollars ($200) for each deletion request for each day the data broker fails to delete information as required by Section 1798.99.86.~~

~~(2) Expenses incurred by the Attorney General in the investigation and prosecution of the action as the court deems appropriate.~~

~~(f)~~ ***(d)*** A data broker required to register under this title that fails to comply with the requirements of Section 1798.99.86 is liable for administrative fines and costs in an administrative action brought by the California Privacy Protection Agency as follows:

(1) An administrative fine of two hundred dollars ($200) for each deletion request for each day the data broker fails to delete information as required by Section 1798.99.86.

(2) Expenses incurred by the California Privacy Protection Agency in the investigation and administration of the action as the court deems appropriate.

~~(g)~~ ***(e)*** Any penalties, fines, fees, and expenses recovered in an action prosecuted under subdivisions (c) ***or*** ~~to~~ (~~f~~***d***)~~, inclusive,~~ shall be deposited in the Data Brokers' Registry Fund, created within the State Treasury pursuant to of Section 1798.99.81, with the intent that they be used to fully offset costs incurred by the state ~~courts,~~ *courts and* the California Privacy Protection ~~Agency, and the Attorney General~~ *Agency* in connection with this title.

~~(h) The California Privacy Protection Agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action, and shall not pursue an administrative action~~

~~or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action.~~

~~(i) (1) The Attorney General shall not file a civil action pursuant to this section after the California Privacy Protection Agency has issued a decision pursuant to this section for the same underlying conduct.~~

~~(2) The California Privacy Protection Agency shall not file an administrative action pursuant to this section after the Attorney General has brought an action pursuant to this section for the same underlying conduct.~~

One note about the amendments above. With these amendments, a single reference to the Department of Justice will remain in the bill, in the first paragraph of Section 1798.99.81. The author's office is working with the Department of Justice and the Privacy Agency on the details of transferring administration of the existing Data Brokers' Registry Fund from the former agency to the latter; it is anticipated the bill will be amended once more to reflect this issue's resolution.

The following amendment would ensure that data brokers compile the number of requests to limit sensitive personal information that they received in the previous year.

1798.99.85. (a) On or before January 31 following each year in which a business meets the definition of a data broker as provided in this title, the business shall do all of the following:

(1) Compile the number of requests pursuant to Sections 1798.105, 1798.110, 1798.115, ~~and~~ 1798.120, ***and 1798.121*** that the data broker received, complied with in whole or in part, and denied.

(2) Compile the median and the mean number of days within which the data broker substantively responded to requests pursuant to Sections 1798.105, 1798.110, 1798.115, ~~and~~ 1798.120***, and 1798.121*** that the data broker received.

(3) Disclose the metrics compiled pursuant to paragraphs (1) and (2) on the data broker's internet website and provide a link to that internet website in the data broker's privacy policy.

(b) In its disclosure pursuant to paragraph (3) of subdivision (a), a data broker shall disclose the number of requests that the data broker denied in whole or in part because of any of the following:

(1) The request was unverifiable.

(2) The request was not made by a consumer.

(3) The request called for information exempt from disclosure.

(4) The request was denied on other grounds.

The following amendments allow a consumer to exclude specific data brokers from their deletion request, and to revoke a previously-made deletion request:

1798.99.86. (a) By January 1, 2026, the California Privacy Protection Agency shall establish an accessible deletion mechanism that does ~~both~~ ***all*** of the following:

(1) Implements and maintains 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 personal information will be used and to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

(2) Allows 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.

(3) Allows a consumer to selectively exclude specific data brokers from a request made under this subdivision.

(4) Allows a consumer to make a request to undo or alter a previous request made under this subdivision after at least 31 days have passed since the consumer last made a request under this subdivision.

The following amendment ensures that statutory authority, for an agent to make a deletion request on a consumer's behalf, is not tied to a reference in the California Code of Regulations, the number of which could change in the future:

1798.99.86. […] (b) The accessible deletion mechanism established pursuant to subdivision (a) shall meet all of the following requirements:

[…]

(8) The accessible deletion mechanism shall support the ability of a consumer's authorized agents to aid in the deletion ~~request pursuant to Section 7063 of Title 11 of the California Code of Regulations.~~ ***request.***

The following amendment clarifies that for data brokers to "process" deletion requests means to delete the personal information of requesting consumers:

1798.99.86 […] (c) (1) Beginning August 1, 2026, a data broker shall access the accessible deletion mechanism established pursuant to subdivision (a) at least once every 31 days and do all of the following:

(A) Process all deletion requests made pursuant to this ***section and delete all personal information related to the consumers making the requests consistent with the requirements of this section.***

The following amendment reduces the compliance burden on data brokers and the administrative burden on the Privacy Agency by requiring that a data broker need only submit audit reports to the Agency only on request (rather than every data broker having to submit reports to the Agency every year):

1798.99.86 […] (e) (1) Beginning January 1, 2028, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance with this section.

(2) ~~By six months after the completion of~~ ***For*** an audit ***completed*** pursuant to paragraph (1), the data broker shall submit a report resulting from the audit and any related materials to the California Privacy Protection Agency ***within five business days of a written request from the California Privacy Protection Agency***.

The following amendment clarifies that the Privacy Agency has the same statutory limitations period—five years— to bring an administrative enforcement action under the DBRL that it does under the CCPA.

1798.99.89. An administrative action brought pursuant to this title shall not be commenced more than five years after the date on which the violation occurred.

11) **Related legislation.** AB 947 (Gabriel, 2023) would add "citizenship or immigration status" to the definition of "sensitive personal information" under the CCPA, affording this information heightened protections. Status: Senate Appropriations Committee.

SB 1059 (Becker, 2022) would have enhanced the DBRL and transferred most of the relevant duties from the Attorney General to the Privacy Agency. Status: Held, Senate Appropriations Committee.

AB 1202 (Chau, Chap. 753, Stats. 2019) enacted the DBRL.

ARGUMENTS IN SUPPORT: A coalition of 20 legal aid groups and consumer rights nonprofits explains the need for this bill:

> [C]oncerns [about data brokers' practices] 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.

ARGUMENTS IN OPPOSITION: A coalition of nine business trade associations explains why this bill is unnecessary:

> [T]his bill makes significant changes to the Data Brokers' Registry and the Data Brokers' Registry Fund, adding extensive disclosure requirements and deletion obligations under the Data Brokers' Registry law, for a subset of businesses that are already subject to the California Consumer Privacy Act (CCPA). With the passage of the CCPA, California was the first state to pass a comprehensive privacy law that applied in an industry neutral manner, and it followed that law with a consumer-facing registry that specifically would enable

consumers to exercise their rights with data brokers. Unfortunately, based on an inaccurate interpretation of existing law, the bill creates a duplicative and potentially confusing regime for companies that are already subject to the CCPA, which already includes disclosures around collection activities and otherwise provides consumers with deletion rights and the ability to opt out of the sale and sharing of [personal information]. We are also very concerned that the bill places new, onerous obligations on the California Privacy Protection Agency…to create an unnecessary deletion mechanism for CCPA-covered businesses that also must register with the Attorney General's Office as a data broker.

REGISTERED SUPPORT / OPPOSITION:

Support

Privacy Rights Clearinghouse (sponsor)
Access Reproductive Justice
Bet Tzedek Legal Services
Calegislation
Californians for Consumer Privacy
CalPIRG
Cameo - California Association for Micro Enterprise Opportunity
Centro Legal De La Raza
Community Legal Services in East Palo Alto
Consumer Action
Consumer Attorneys of California
Consumer Federation of America
Consumer Reports
Consumer Watchdog
Electronic Frontier Foundation
Electronic Privacy Information Center
Encode Justice
Fairplay
Katharine & George Alexander Community Law Center
Legal Aid of Marin
Legal Aid Society of San Bernardino
Legal Assistance for Seniors
Oakland Privacy
Open Door Legal
Planned Parenthood Affiliates of California
Public Counsel
Public Law Center
Riverside Legal Aid
Ultraviolet Action
Watsonville Law Center

Opposition

American Advertising Federation
American Association of Advertising Agencies
Association of National Advertisers

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 & Security Coalition
TechNet

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200