Date of Hearing: June 24, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 361 (Becker) – As Amended March 24, 2025

PROPOSED AMENDMENTS

SENATE VOTE: 37-0

SUBJECT: Data broker registration: data collection

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. In 2023, this was further amended by SB 362 (Becker, Chap. 709, 2023) to create a streamlined process for consumers to exercise their right to delete data held by data brokers as well as mandate that data brokers must disclose whether they collect data on reproductive health or precise geolocation.

Nevertheless, fears have continued to rise about the types of information that data brokers collect and whether that information can be used punitively. Recent reporting in Colorado suggests that Immigration and Customs Enforcement (ICE) has used information collected by data brokers to circumvent sanctuary state laws.

This bill, sponsored by Oakland Privacy, expands the types of information that data brokers must disclose that they collect which will then be displayed on the data broker registry. Specifically, it requires data brokers to indicate whether they are collecting account logins and account numbers, driver's license numbers and other types of identification numbers, citizenship data, union membership data, sexual orientation data, gender identity and expression information, and biometric information. This bill is supported by the California Federation of Labor Unions and Secure Justice.

Committee Amendments described in Comment #5 would increase transparency by requiring data brokers to disclose when registering whether they have sold or shared consumers' information with a foreign actor, the federal government, other state governments, a law enforcement agency, or a developer of an AI system or model in the past year.

THIS BILL:

1) Requires data brokers registering with the California Privacy Protection Agency (Privacy Agency) to indicate whether they collect the following information on consumers:

a) Account login or account number in combination with any required security code, access code, or password that would permit access to a consumer's account with a third party;

b) Drivers' license number, California identification card number, tax identification number, social security number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

c) Citizenship data, including immigration status;

d) Union membership status;

e) Sexual orientation status;

f) Gender identity and gender expression data; or

g) Biometric data.

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 Privacy Agency, as provided. (Civ. Code § 1798.99.82.)

2) Defines "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The definition specifically excludes the following:

    a) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

    b) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations; and

    c) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act, Insurance Code § 1791 et seq. (Civ. Code § 1798.99.80.)

3) Aligns the definitions of "business," "personal information," "sale," "collect," "consumer," and "third party" with those in the Privacy Agency. (Civ. Code § 1798.99.80.)

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

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

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

7) Provides that after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant hereto, the data broker must delete all personal information of the consumer, except as provided, beginning August 1, 2026. After a consumer has submitted a deletion request and a data broker has deleted the consumer's data, the data broker shall not sell or share new personal information of the consumer unless the consumer requests otherwise or the selling or sharing of the information is otherwise permitted, as provided. Requires data brokers to undergo audits every three years to determine compliance with the data broker registry law. (Civ. Code § 1798.99.86.)

8) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

9) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the Privacy Agency, which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

10) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

11) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the following:

    a) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;

    b) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive

personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and

c) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose. (Civ. Code § 1798.100(a).)

12) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

a) The categories of personal information it has collected about that consumer;

b) The categories of sources from which the personal information is collected;

c) The business or commercial purpose for collecting, selling, or sharing personal information;

d) The categories of third parties with whom the business shares personal information; and

e) The specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

13) Provides consumers the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer specified information, including the categories of personal information collected, shared, sold, and disclosed and the categories of third parties receiving the information. (Civ. Code § 1798.115.)

14) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of the sale or sharing of their personal information. (Civ. Code § 1798.120.)

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

16) Defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including

biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

17) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as genetic data and the processing of biometric information for the purpose of uniquely identifying a consumer. (Civ. Code § 1798.140(ae).)

18) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

19) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

COMMENTS:

1) **Author's statement**. According to the author:

> Californians have a right to know who is collecting their most sensitive personal information. SB 361 increases transparency in the data broker industry, helping people protect their privacy.
>
> There are serious concerns that data brokers are selling sensitive information in ways that could lead to surveillance and targeting of vulnerable communities, including immigrants, and LGBTQ+ individuals. The risks of mass deportation, discrimination, and other harmful outcomes are real, and we must act to protect people's privacy.
>
> Building on the California Delete Act, which was passed in 2023, SB 361 requires data brokers to disclose whether they collect sensitive information like government IDs, union membership, and sexual orientation. The California Privacy Protection Agency (CPPA) will publish this information, empowering Californians to make informed decisions about their privacy and will soon have the ability with the click of a single link to delete their personal data and prevent it from being sold.
>
> California has long been a leader in privacy protections, and SB 361 ensures that individuals—not data brokers—remain in control of their personal information.

2) **The Commodification of Personal Data**. Enshrined in the state constitution by a ballot initiative in 1972, the unalienable right to privacy is guaranteed to all Californians and is enforceable against both the public and private sectors. However, for the past 20 years, experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted in *The Guardian* a decade ago:

> We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . .

> Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.[1]

Since this piece was published, it has become increasingly clear that not only is our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff. In an opinion piece for *The New York Times,* in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .
>
> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[2]

The rapid advancement of artificial intelligence over the past five years has significantly accelerated data collection and processing. AI agents can be deployed to extract data, also known as scraping, from websites. Inevitably this includes personal information about consumers which data brokers compile and sell to businesses. These businesses then integrate the acquired data with their own consumer information to create detailed consumer profiles. With AI, these profiles can be updated in real time to personalize user experiences and target advertisements more effectively.

3) **Why protecting personal information is important**. Some may consider sharing their private information, including websites they visit, purchases, employment history, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, failing to actively protect our private information can have real world consequences. As an example, dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal information with advertisers, including location, sexual orientation and mental health details.[3] This was not the first time Grindr had failed to protect their users' private information. Several years earlier, it

---

[1] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014), https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.
[2] Zuboff, Shoshana. "You Are the Object of a Secret Extraction Operation." *The New York Times* (Nov. 12, 2021) *available at* https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[3] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.

was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[4]

More recently, a hack of the location data analytics company Gravy Analytics revealed that precise geolocation data was being collected from thousands of apps, including Candy Crush, Tinder, and even many VPN apps, which ironically are intended to enhance user privacy.[5] The hack exposed that app developers themselves were often unaware of this tracking, as the data was gathered through advertisements embedded in the apps. Gravy Analytics aggregated this geolocation data and sold it to advertisers and government entities, including the U.S. federal government. The fact that this data was collected without the knowledge of either users or developers underscores serious concerns about the reach and practices of data brokers.

Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), consumers are granted a range of privacy protections, including the right to transparency, notice, correction, deletion, and the ability to opt out of data collection. However, enforcing these rights has proven challenging due to the opaque practices of data brokers like Gravy Analytics. These entities rarely interact directly with consumers. Instead, they collect data by partnering with businesses, purchasing data from other brokers, or scraping the internet to compile detailed consumer profiles. This creates a system in which consumers are unaware that their data is being collected, let alone what data is being held or where it came from. In December, the Federal Trade Commission (FTC) took enforcement action against Gravy Analytics, alleging the company had sold non-anonymized location data in violation of consumer protection standards, resulting in a prohibition in the selling and sharing of sensitive location data.[6]

California has made strides to address this lack of transparency. AB 1202 (Chau, Ch. 753, Stats. 2019) established the state's data broker registry, requiring brokers to register and disclose certain practices. Brokers must now report if they collect sensitive categories such as precise geolocation or reproductive health data. Yet, for most consumers, it remains nearly impossible to know what personal information is being collected or how it may be used.

This lack of visibility is especially concerning when data broker information can be used punitively. For example, recent increases in U.S. Immigration and Customs Enforcement (ICE) activity have raised alarms about the use of brokered data to bypass sanctuary laws, an issue already documented in Colorado.[7] Employers could potentially access brokered data to discriminate against job applicants with a history of union involvement. Similarly, data revealing gender identity or sexual orientation could be exploited to harass, intimidate, or dox individuals.

---

[4] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
[5] Joseph Cox, "Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location", *Wired* (Jan. 9, 2025), https://www.wired.com/story/gravy-location-data-app-leak-rtb/.
[6] Federal Trade Commission, "FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data" (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-gravy-analytics-venntel-selling-sensitive-location-data.
[7] Johana Bhuiyan, "US immigration agency explores data loophole to obtain information on deportation targets", *The Guardian* (Apr. 20, 2022), https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets.

To help address these risks, SB 362 (Becker, Ch. 709, Stats. 2023) strengthened consumers' rights by establishing a centralized data deletion mechanism. Beginning in 2026, consumers will be able to submit a single deletion request form, requiring all registered brokers to delete their personal information, and to continue deleting any new data collected every 45 days thereafter. The law also requires brokers to disclose whether they are regulated under specific state and federal laws and to include this information on the California Privacy Protection Agency's website. Beginning in 2028, data brokers will also be subject to third-party audits to verify compliance with SB 362.

Despite these advances, consumers still deserve a clear understanding of what types of sensitive information are being collected and traded by data brokers, and how that information could potentially be used against them.

4) **What this bill would do.** This bill expands the categories of data that data brokers must disclose to the California Privacy Protection Agency during their annual registration. Specifically, it requires data brokers to report whether they collect account login credentials or account numbers in combination with any required security code, access code, or password that would allow access to a consumer's account with a third party. In addition, brokers must disclose if they collect highly sensitive information such as government-issued ID numbers (including driver's license, Social Security, and tax identification numbers), citizenship status, union membership, sexual orientation, gender identity, and biometric data. As noted above, this type of information has become increasingly sensitive due to its weaponization by ICE against immigrants, both documented and undocumented, as well as U.S. citizens.

These new disclosure requirements build upon SB 362, which mandated transparency around the collection of minors' personal information, reproductive health data, and precise geolocation. Beyond improving transparency, this bill serves as a reminder of the growing reach of the surveillance state and the risks posed when sensitive consumer data is collected and potentially used for punitive purposes.

5) Committee Amendments. The current bill focuses on requiring data brokers to disclose the types of information they collect. However, it does not enhance transparency around where that data is sold or shared. This is a significant gap, particularly if consumer data is being transferred to foreign entities, law enforcement, or other actors who could misuse it. Providing consumers with more visibility into how their data is used, and with whom it is shared or sold, would better enable them to exercise their right to request deletion of their personal information.

To address this concern, the author has agreed to amend the bill to require data brokers, as part of their annual registration, to disclose whether they have sold or shared consumer information within the past year with:

1. A foreign actor,
2. The federal government,
3. Other state governments,
4. A law enforcement agency, or
5. A developer of an artificial intelligence system or model.

The full text of the amendments is provided below:

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.

(b) In registering with the California Privacy Protection Agency, as described in subdivision (a), a data broker shall do all of the following:

(1) Pay a registration fee in an amount determined by the California Privacy Protection Agency, not to exceed the reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84 and the reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in Section 1798.99.86. Registration fees shall be deposited in the Data Brokers' Registry Fund, created within the State Treasury pursuant to Section 1798.99.81, and used for the purposes outlined in this paragraph.

(2) Provide the following information:

(A) The name of the data broker and its primary physical, email, and internet website addresses.

(B) The metrics compiled pursuant to paragraphs (1) and (2) of subdivision (a) of Section 1798.99.85.

(C) Whether the data broker collects the personal information of minors.

(D) Whether the data broker collects consumers' account login or account number in combination with any required security code, access code, or password that would permit access to a consumer's account with a third party.

(E) Whether the data broker collects consumers' drivers' license number, California identification card number, tax identification number, social security number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(F) Whether the data broker collects consumers' citizenship data, including immigration status.

(G) Whether the data broker collects consumers' union membership status.

(H) Whether the data broker collects consumers' sexual orientation status.

(I) Whether the data broker collects consumers' gender identity and gender expression data.

(J) Whether the data broker collects consumers' biometric data.

(K) Whether the data broker collects consumers' precise geolocation.

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

(M) Whether the data broker has shared or sold consumers' data to a foreign actor in the past year.

(N) Whether the data broker has shared or sold consumers' data to the federal government in the past year.

(O) Whether the data broker has shared or sold consumers' data to other state governments in the past year.

(P) Whether the data broker has shared or sold consumers' data to law enforcement in the past year.

(Q) Whether the data broker has shared or sold consumers' data to a developer of an AI system or model in the past year.

(~~M~~***R***) Beginning January 1, 2029, whether the data broker has undergone an audit as described in subdivision (e) of Section 1798.99.86, and, if so, the most recent year that the data broker has submitted a report resulting from the audit and any related materials to the California Privacy Protection Agency.

(~~N~~***S***) A link to a page on the data broker's internet website that does both of the following:

(i) Details how consumers may exercise their privacy rights by doing all of the following:

(I) Deleting personal information, as described in Section 1798.105.

(II) Correcting inaccurate personal information, as described in Section 1798.106.

(III) Learning what personal information is being collected and how to access that personal information, as described in Section 1798.110.

(IV) Learning what personal information is being sold or shared and to whom, as described in Section 1798.115.

(V) Learning how to opt out of the sale or sharing of personal information, as described in Section 1798.120.

(VI) Learning how to limit the use and disclosure of sensitive personal information, as described in Section 1798.121.

(ii) Does not make use of any dark patterns.

(~~O~~***T***) Whether and to what extent the data broker or any of its subsidiaries is regulated by any of the following:

(i) The federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(ii) The Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(iii) The Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

(iv) The Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).

(~~P~~***U***) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(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.

(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) Reasonable expenses incurred by the California Privacy Protection Agency in the investigation and administration of the action.

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

(f) For the purpose of this section, the following terms are defined:

(1) "Foreign agents" means either of the following:

(A) The government of a foreign country.

(B) A partnership, association, corporation, organization, or other combination of persons organized under the laws of or having its principal place of business in a foreign country.

(2) "Developer of an AI system or model" means a person, partnership, state or local government agency, or corporation that designs, codes, produces, or substantially modifies an artificial intelligence system or service for use by members of the public.

ARGUMENTS IN SUPPORT: Oakland Privacy, the sponsor of the bill, write in support:

The premise of SB 361 is that Californians have a right to know which companies have obtained and are prepared to sell their highly sensitive information and to be able to distinguish those particular data brokers from those who are distributing less sensitive information. We absolutely agree that both consumers and regulators should have access to this information, and most importantly, that gaining that access should not be a burdensome process for consumers.

The bill requires data brokers to disclose when they register whether or not they collect certain kinds of specific information that can be considered sensitive or high-risk for the individuals in their databases including:

- log-in data like user names, passwords, and account numbers

- governmental identifier numbers like social security numbers, drivers license numbers or military IDs

- citizenship data and immigration status

- information about sexual orientation and identity

- information about union membership and activism

- biometric data including faceprints, iris prints, palm prints, voiceprints, gait indicators and neural data.

Sensitive or high risk data is information that consumers need to protect for specific reasons, which can include identity theft and identity verification, as well as potentially negative ramifications if information sold by third parties gets into the wrong hands including blackmail, threats to employment and deportation.

The initial iteration of the registry asks the data broker registrants three questions about what they collect: whether they collect the information of minors, whether they collect geolocation data, and whether they collect data about reproductive health care. SB 361 would ask the same questions about six more categories of sensitive information which are listed above.

While the DROP mechanism is intended to allow Californians to opt out from all registered data broker data sales and profiling, the additional information that would be provided by the bill would be helpful to consumers in several ways:

1. To focus on the particular companies that collect personal information they are particularly worried about safeguarding and ensure that the DROP process worked for them if they chose to use it.

2. To motivate consumers to use the DROP service if they need it, by helping them to understand in more specificity what kinds of personal information is being collected and is potentially being sold.

3. To assist regulators and legislators to have a better understanding of the specifics of data broker marketplaces and to identify and address new risks as they develop as

technology continues to innovate, creating new methodologies for the use and misuse of sensitive personal information.

We don't believe that the additional information that would be added to the data broker registration process is particularly burdensome to the companies. They know what they collect. It is only the consumer who doesn't know this information.

REGISTERED SUPPORT / OPPOSITION:

Support

California Community Foundation
California Federation of Labor Unions, Afl-cio
California Initiative for Technology & Democracy, a Project of California Common CAUSE
California Nurses Association
California Privacy Protection Agency
Consumer Federation of California
Consumer Reports
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Oakland Privacy
Privacy Rights Clearinghouse
Puente De LA Costa Sur
Secure Justice

Opposition

None on file.

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200