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

SB 1076 (Wilk)
Version: February 12, 2024
Hearing Date: April 23, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Data brokers: accessible deletion mechanism

DIGEST

This bill amends the recently enacted Delete Act by imposing a series of requirements on consumers and their authorized agents before they can effectively exercise their rights with respect to personal information held by data brokers.

EXECUTIVE SUMMARY

Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection provides consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of California's Constitution. One particularly troubling area of this systematic data collection is the emergence of data brokers that collect and profit from this data without having any direct relationship with the consumers whose information they amass.

In order to bring this industry into the light and more fully inform consumers about who is collecting their personal information and how, a data broker registry was established in California law requiring data brokers to register annually with the Attorney General. Data brokers are required to pay a fee and provide basic information about them. Responding to concerns that existing law did not do enough to bring this industry into the light and to provide consumers more control over their personal information, SB 362 (Becker, Ch. 709, Stats. 2023) established the Delete Act, which bolstered the data broker registry law by, in part, requiring more information to be reported and transferring much of the relevant duties from the Attorney General to the California Privacy Protection Agency (PPA). More importantly, it also expanded consumers' deletion rights and requires the PPA to create an accessible deletion mechanism that allows a consumer, through a single request, to request that every data broker delete the personal information related to the consumer and held by the data

broker, except as specified. To ensure consumers can meaningfully exercise their rights under the law given the hundreds of data brokers on the registry, the mechanism is required to support the ability of a consumer's authorized agent to aid in the deletion request. This is critical as there are currently 550 data brokers registered in California.

This bill creates a series of hurdles for consumers looking to exercise their rights under the Act, including additional steps to request deletion and utilize authorized agents. The bill also removes the provision that treats requests that cannot be verified as an automatic "opt-out request," thereby allowing these data brokers to continue to sell consumers' information.

The bill is co-sponsored by the Credit Builders Alliance and the Consumer Data Industry Association. It is supported by the Network Advertising Initiative. It is opposed by Privacy Rights Clearinghouse, the sponsor of last year's Delete Act legislation, as well as a long list of other advocacy organizations and institutions, including the Public Law Center, the Katharine & George Alexander Community Law Center at Santa Clara Law and Consumer Reports.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Requires a business, on or before January 31 following each year in which it meets the definition of a data broker, to register with the PPA, as provided. (Civ. Code § 1798.99.82.)

2) Defines "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The definition specifically excludes the following:
    a) a consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
    b) a financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations; and
    c) an entity to the extent that it is covered by the Insurance Information and Privacy Protection Act, Insurance Code § 1791 et seq. (Civ. Code § 1798.99.80.)

3) Requires data brokers, when registering, to provide various pieces of information, including:
    a) whether the data broker collects data of minors; precise geolocation data; or reproductive health care data; and
    b) a link to a website that includes details on how consumers may exercise their rights to delete personal information, correct inaccurate personal information, know what personal information is being collected, sold, or

shared, and how to access it, how to opt-out of the sale or sharing of personal information, and how to limit the use and disclosure of sensitive personal information. (Civ. Code § 1798.99.82.)

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

5) Requires data brokers, in cases where they deny a consumer request to delete because the request cannot be verified, to process the request as an opt-out of the sale or sharing of the consumer's personal information. (Civ. Code § 1798.99.86.)

6) Authorizes the PPA to adopt regulations in compliance with the Administrative Procedure Act. (Civ. Code § 1798.99.87.)

7) Authorizes administrative actions to be brought against data brokers in violation of the law by the PPA and provides for administrative fines of $200 for specific violations. (Civ. Code § 1798.99.82.)

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

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

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

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

12) Provides that a business or service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business or service

provider to maintain the consumer's personal information in order to do certain things, including to comply with a legal obligation. (Civ. Code § 1798.105(d).)

13) 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.)

14) 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).)

15) 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).)

16) 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).)

17) 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.)

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

This bill:

1) Imposes the following requirements on the accessible deletion mechanism's support of authorized agents:
    - An authorized agent shall not aid in a deletion request unless the authorized agent is registered with, and certified by, the PPA.

- Consumer requests made by an authorized agent shall be subject to Section 7063 of Title 11 of the California Code of Regulations.
- Data broker processing of requests made by an authorized agent shall be subject to Section 7063 of Title 11 of the California Code of Regulations.
- An authorized agent shall ensure that the consumer is reasonably informed about a deletion decision and the rights granted to the consumer by the Delete Act.
- An authorized agent shall facilitate the consumer's exercise of any rights granted to the consumer.
- An authorized agent shall not sell, share, or use, or act on behalf of or in concert with an entity that sells, shares, or uses personal information to deliver advertising and marketing services to another business.
- An authorized agent shall not charge the consumer a fee, or act on behalf of or in concert with an entity that charges the consumer a fee, to facilitate a deletion request.
- If an authorized agent submits a consumer's email as part of a deletion request, the email address shall allow the data broker to directly contact the consumer without an authorized agent.

2) Requires the accessible deletion mechanism to include sufficient information for a data broker to directly contact the consumer in a manner that is substantially similar to the manner the consumer used to request the deletion.

3) Requires the accessible deletion mechanism to include procedures to authenticate to a high level of certainty the identity of a consumer who submits a deletion request that comply with industry and government best practices and standards for identity verification, assurance, and fraud protection.

4) Deletes the provision requiring data brokers that deny a consumer request to delete because the request cannot be verified to treat the request as an opt-out of the sale or sharing of the consumer's personal information.

5) Authorizes data brokers, when accessing the deletion mechanism, to do the following:
    - When denying a request for verification purposes, the data broker can ask the consumer if they want them to treat the request as an opt out. The data broker can then ask the consumer for information necessary to complete the request, including, but not limited to, information necessary to identify the consumer, and must direct all service providers or contractors associated with the data broker to process the request in the same manner as the data broker.
    - Deny the request if the data broker has a good faith, reasonable, and documented belief that the request is fraudulent.

i. If a data broker denies such a request, the data broker shall inform the consumer that the data broker will not comply with the request and provide an explanation describing why the data broker believes the request is fraudulent.

- Deny the request if the request was submitted through an authorized agent and the agent has not provided the consumer's signed permission demonstrating that the authorized agent has the authority to act on the consumer's behalf.

6) Requires, instead of authorizes, the PPA to issue regulations to implement the Delete Act by August 1, 2025 pursuant to the Administrative Procedure Act.

7) Provides that the Legislature finds and declares that this act furthers the purposes and intent of the CPRA by ensuring consumers' rights, including the constitutional right to privacy, are protected by enacting additional consumer protection provisions regarding consumers' requests that data brokers delete their personal information, including additional safeguards related to consumers' use of authorized agents to make those requests.

COMMENTS

1. Growth of the data broker industry

Consumers' web browsing, online purchases, and involvement in loyalty programs create a treasure trove of information on consumers. Many applications on the smartphones that most consumers carry with them throughout the day can track their every movement.

The information economy has given rise to the data broker industry, whose business model is built on amassing vast amounts of information through various public and private sources and packaging it for other businesses, and even government entities, to buy. The collection of this data combined with advanced technologies and the use of sophisticated algorithms can create incredibly detailed and effective profiling and targeted marketing from this web of information.

A report by the Federal Trade Commission (FTC) found that data brokers "collect and store a vast amount of data on almost every U.S. household and commercial transaction," most of them "store all data indefinitely," and that "many of the purposes for which data brokers collect and use data pose risks to consumers."[1]

[1] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. All internet citations are current as of April 17, 2024.

The Electronic Privacy Information Center has detailed its concerns with the secrecy and depth of the industry:

> Data brokers use secret algorithms to build profiles on every American citizen, regardless of whether the individual even knows that the data broker exists. As such, consumers now face the specter of a "scored society" where they do not have access to the most basic information on how they are evaluated. The data broker industry's secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs. In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage. Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[2]

Consumers have expressed growing concern in response to this profiling. A study by the Pew Research Center found that 68 percent of American Internet users believe existing law does not go far enough to protect individual online privacy, with only 24 percent believing current laws provide reasonable protections.[3]

2. California's data broker registry

California has responded to these concerns with a number of state laws that seek to provide transparency, control, and accountability in the information economy.

The CCPA, amended by the CPRA, grants a set of rights to consumers with regard to their personal information, including enhanced notice and disclosure rights regarding information collection and use practices, access to the information collected, the right to delete certain information, the right to restrict the sale of information, and protection from discrimination for exercising these rights. The CPRA also added in additional protections for "sensitive personal information."

Although these are ground-breaking rights for consumers to protect their right to privacy, many of the provisions require consumers to know which entities have their personal information before they can properly exercise their rights. The data brokers discussed above, by definition, do not have direct relationships with consumers and can essentially amass personal information on consumers without their permission or knowledge. As found by the FTC, "because data brokers are not consumer-facing, consumers may not know where to go to exercise any choices that may be offered." The FTC report elaborated:

---

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

> Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

That FTC report further found that the attenuated connection to consumers is only further exacerbated by the fact that most data brokers obtained enormous amounts of data from other data brokers: "The data broker industry is complex, with multiple layers of data brokers providing data to each other." The FTC found that it would be "virtually impossible for a consumer to determine how a data broker obtained [their] data; the consumer would have to retrace the path of data through a series of data brokers."

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

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

To begin to address these concerns, AB 1202 (Chau, Ch. 753, Stats. 2019) established California's data broker registry. The bill was modeled on a Vermont law, Vt. Stat. Ann. tit. 9, §§ 2446 et seq., and requires data brokers to register with, and pay a registration fee to, the Attorney General on an annual basis. The law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."

In order to address some gaps in the law and ensure that consumers can effectively enforce their rights under it, SB 362 (Becker, Ch. 709, Stats. 2023) was signed into law, establishing the Delete Act. It bolstered the utility and effectiveness of the existing data broker registry law in myriad ways and strengthened consumers' right to deletion as to data brokers.

The act requires more detailed information to be provided by data brokers and to be included with the other registration information on the PPA's website. Data brokers are

required to disclose whether and to what extent they are regulated under specified state and federal laws. It also requires data brokers to disclose whether they collect personal information from children and whether they collect consumers' precise geolocation or reproductive health care data. This provides greater clarity for consumers on whether this especially sensitive information is being collected by a particular broker.

Data brokers must also provide a link to a page on the data broker's internet website that details how consumers can exercise their CPRA rights, including how to: learn what personal information is being collected; access that personal information; delete their personal information; correct inaccurate personal information; learn what personal information is being sold or shared, and to whom; learn how to opt out of the sale or sharing of personal information; and limit the use and disclosure of sensitive personal information. The site is explicitly restricted from making use of dark patterns.

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

3. Short-circuiting the streamlined processes of the Delete Act

Most relevant here, the Delete Act requires the PPA to establish an "accessible deletion mechanism" that is capable of doing both of the following:

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

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

Data brokers are required to regularly access the system securely and process all pending deletion requests. They are further required to direct their service providers or contractors to also delete all such personal information.

A mechanism of this sort provides a much greater degree of control to consumers over their personal information. First, it is largely impractical for a consumer to navigate the systems of the hundreds of data brokers and to submit deletion requests individually to each. This allows a consumer to delete their information with a single, secure request. Just as with the CPRA, there are exceptions allowing for brokers to retain personal information where necessary, for instance, to comply with a warrant or other applicable law or for the exercise of free speech.

The PPA has until January 1, 2026 to establish this accessible deletion mechanism that meets the stated security and operability requirements. Brokers are required to start accessing it to process requests in August 2026.

Despite the ongoing development of this mechanism, this bill now seeks to impose a series of new requirements on the mechanisms that consumers can use to exercise their rights pursuant to the Act. The bill places additional requirements that the mechanism provide brokers information so that they can directly contact consumers before requests are processed. The bill also raises the threshold for authentication.

Currently, if a data broker denies a request to delete because the request cannot be verified, the broker must treat the request as an opt-out of the sale or sharing of the consumer's data. This ensures that where a consumer unsuccessfully seeks deletion, they are still afforded this basic protection that does not require full deletion. This bill eliminates this protection. The bill also provides data brokers an additional basis to deny requests if they have a good faith, reasonable, and documented belief that the request is fraudulent.

One key provision of the Delete Act provides that the accessible deletion mechanism must support the ability of a consumer's authorized agent to aid in deletion requests. This provides consumers the ability to rely on these agents to undertake the arduous process of exercise their deletion rights with respect to the 550 data brokers currently registered in California.

This bill now subjects requests made by authorized agents to a series of onerous requirements. This includes that authorized agents must themselves register with the PPA. The agents are also prohibited from charging a consumer a fee. If an authorized agent submits a consumer's email as part of a deletion request, the bill requires the email address to allow the data broker to directly contact the consumer without an authorized agent.

According to the author:

> Since 2020, data brokers have been required to register and disclose certain information about consumer privacy rights. While data brokers are narrowly defined to cover a business that does not have a direct

> relationship with consumers and sells consumer personal information to third parties, the registry is compiled of a diverse set of companies providing business and consumer services. In 2023, the legislature approved SB 362 to expand disclosures for registered data brokers and required the Consumer Privacy Protection Agency to establish a mechanism for consumers or their authorized agents to make a one-stop deletion request to all registered data brokers. The creation of a one-stop data deletion mechanism for registered data brokers provides consumers with a centralized deletion request for over 500 registered companies. While the mechanism is intended to allow greater consumer privacy options, the mechanism, as established, is at risk for abuse. . . .
>
> While the deletion mechanism does not charge a consumer, there is no limitation on third party services, or authorized agents, to charge consumers in order to facilitate deletion through the mechanism. The ability of third parties to charge for otherwise free government services opens the door to unscrupulous actors.
>
> The deletion mechanism also raises anticompetitive concerns as the data broker registry does not capture all businesses in a similar competitive market. As a result, the mechanism could be used by non-data brokers to drive deletion requests and gain a competitive advantage.
>
> The deletion mechanism does not go into effect until 2026, providing the legislature the opportunity to resolve critical consumer protection issues. SB 1076 represents the opportunity to these issues before the mechanism is established.

A coalition of organizations including Santa Clara Law's Community Law Center, Public Law Center, the California Low Income Consumer Coalition, and others, write in opposition to the bill:

> Under the California Consumer Privacy Act (CCPA) consumers have been unable to exercise their right to deletion when it comes to data brokers; and due to the sheer scale of the industry (with 405 registered with the California Privacy Protection Agency as of March, 2024) consumers face an insurmountable challenge to repeatedly exercise the CCPA rights that do apply to their personal information held by data brokers on a business-by-business basis.
>
> Thankfully, last year, the Legislature took a monumental step forward in passing SB 362, the California Delete Act, which is poised to empower Californians with the tools necessary to protect their personal information from data brokers. Unfortunately, Senate Bill 1076 (SB 1076) threatens to

gut key parts of that framework before the Delete Act can fully take effect. We strongly urge a NO vote on SB 1076 for the following reasons:

- **SB 1076's Email-Back Provisions Defeat the Very Purpose of the California Delete Act's Streamlined Deletion Process**: SB 1076 introduces barriers to the streamlined deletion process promised by the Delete Act, making it more difficult, if not impossible, for consumers to efficiently exercise their privacy rights.
- **SB 1076 Strips Californians of Power to Exercise Rights and Compromises Privacy for Vulnerable Populations**: SB 1076 places undue burdens on individuals, particularly those who may rely on authorized agents, to navigate an unnecessarily complex deletion process.
- **SB 1076 Seeks Redundant Fraud Prevention Measures**: The bill imposes excessive verification requirements that, at best, are duplicative of existing requirements and at their worst complicate and undermine the deletion process without effectively addressing fraud.
- **SB 1076 Proposes Changes More Appropriately Handled by CPPA Rulemaking**: The bill attempts to bypass the CPPA's established rulemaking process. SB 1076 undermines the CPPA's ability to adapt regulations to evolving privacy challenges, suggesting changes all better addressed through rulemaking.
- **SB 1076 Increases Risks to Consumers of Fraud and Abuse**: By hindering access to deletion mechanisms, SB 1076 facilitates misuse of personal information leading to identity theft, stalking, and harassment. These risks are particularly acute for those seeking reproductive healthcare, gender-affirming care, and low-income communities.
- **SB 1076 Misrepresents Legislative Intent**: The bill misconstrues the purpose of the Delete Act, which targets data brokers due to the unique risks posed by their indirect relationship with consumers. By incorrectly framing the Act as targeting "data aggregators," SB 1076 undermines the legislative framework designed to regulate data brokers under the California Consumer Privacy Act (CCPA).
- **SB 1076 Seeks to Make Changes Already Considered and Rejected by the 2023 Legislature**: SB 1076 attempts to relitigate decisions made by the 2023 legislature disregarding their clear intention to provide Californians with a more accessible, efficient, and effective means of controlling their personal information.
- **SB 1076 Is Unnecessary for Credit Building Services**: The bill's proposed amendments to protect credit building services are redundant, as the Delete Act and CCPA already include balanced

> exemptions for these entities and allow consumers to selectively exclude trusted data brokers from deletion.
>
> The California Delete Act was a landmark achievement designed to empower consumers and help protect their data from misuse. SB 1076 undermines these protections, and we respectfully urge you to oppose.

However, the author argues these changes are necessary to combat fraud:

> Current law does not provide adequate guardrails to protect consumers from potential misuse of the deletion mechanism, such as requirements to authenticate deletion requests from consumers or their authorized agents. Fraudulent or unintended deletion of data establishes a scenario where consumers may have difficulty with access to essential services.
>
> The deletion of data is permanent, with no reasonable way for a consumer to opt back into specific services.

Writing in support, the Credit Builders Alliance echoes this sentiment:

> SB 1076 will also provide protections against misuse of the deletion system that are essential to any framework that gives consumers control over their personal data. Currently, there are not clear requirements that a consumer, or their authorized agent, is authenticated prior to requesting deletion. Without authenticating a consumer request there is significant risk that mechanism could process fraudulent requests. SB 1076 provides the opportunity for the CPPA to develop authentication measure and receive broad stakeholder input through a rulemaking process.

In response, Privacy Rights Clearinghouse and the Electronic Frontier Foundation assert that the Delete Act already includes robust fraud prevention measures:

> Proponents of SB 1076 argue that the heightened individualized authentication and ability to communicate directly with consumers using the mechanism is necessary to prevent fraudulent deletion requests, either by criminals or competing businesses. This is incorrect because security and fraud considerations are built into the Delete Act and required in the design of the accessible deletion mechanism.
>
> The first requirement of the accessible deletion mechanism, in 1798.99.86(a)(1), is that it "[i]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." This is further reinforced in 1798.99.86(b)(3) and 1798.99.86(c)(3)8. Proponents of SB 1076 will have the opportunity to raise their suggestions and share their perspective with the California Privacy Protection Agency as it develops the deletion mechanism.
>
> In addition, the Delete Act permits a data broker to refuse to delete a consumer's information if it is reasonably necessary to fulfill any purpose outlined in the CCPA's Section 1798.105(d) (which limits the Right to Delete). This includes an exemption if the broker can claim the information is reasonably necessary and limited to help ensure security and integrity, a defined term under the CCPA.
>
> Proponents of SB 1076 have not offered any evidence that deletion or authorized agent fraud is a documented problem, and have not offered explanations as to why a criminal would be incentivized to delete a person's data from a data broker (particularly considering the existing exemptions). Authorized agents are not a new concept, and the CCPA was designed to give consumers the choice to use their services. According to responses we obtained from the California Privacy Protection Agency through Public Records Act requests, the agency has received no complaints regarding fraudulent deletion activities or misuse of personal information by authorized agents, as defined in § 7001 of the CCPA Regulations. This includes any breaches of § 7063(c)'s requirement for authorized agents to maintain reasonable security procedures, or violations of § 7063(d), which restricts the use of a consumer's personal information solely to fulfilling the consumer's requests, verification, or fraud prevention.

The Consumer Data Industry Association writes in support:

> SB 1076 also aims to safeguard against the misuse of the deletion system, a critical component of any framework granting consumers control over their personal data. Under the Deletion Act, there is a risk that an optout request might inadvertently affect other consumers who share similar contact information or belong to the same household. This could result in data being opt outed for Californians that did not make the original deletion request or intend to exercise an opt-out, thereby removing their rights under the law. Unfortunately, under current legislation, there is no provision for consumers to reverse an opt-out decision or determine which of the nearly 500 data brokers they should contact.

The Network Advertising Initiative (NAI) is a self-regulatory association focused on data collection and use for digital advertising, with approximately one-third of their members being registered data brokers. NAI writes in support:

> Unfortunately, as enacted, the Delete Act creates a substantial risk that data brokers registered with the CPPA will be exposed to fraudulent and abusive deletion requests through the Mechanism. Specifically, the Act contains an element first created in the CCPA to recognize consumer requests submitted through "authorized agents," or private entities working on behalf of a consumer. NAI members are concerned that the Act does not currently require any form of vetting or verification of authorized agents to ensure that they are legitimate businesses working on behalf of consumers they are claiming to act on behalf of. This could result in individuals or entities posing as authorized agents and purporting to act on behalf of a consumer making fraudulent deletion requests through the Mechanism.

SUPPORT

Consumer Data Industry Association
Credit Builders Alliance
Network Advertising Initiative

OPPOSITION

Abine, Inc. dba Deleteme
California Low-income Consumer Coalition
Californians for Consumer Privacy
CALPIRG
Consumer Attorneys of California
Consumer Federation of California
Consumer Reports
Elder Law & Advocacy
Electronic Frontier Foundation
Fight for The Future
Housing and Economic Rights Advocates (HERA)
LGBT Technology Partnership & Institute
Oakland Privacy
Privacy Rights Clearinghouse
Public Law Center
Santa Clara Law

RELATED LEGISLATION

Pending Legislation: AB 3204 (Bauer-Kahan, 2024) requires data digesters to register with the PPA, pay a registration fee, and provide specified information. "Data digesters" are businesses that use personal information to train artificial intelligence. AB 3204 is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

SB 362 (Becker, Ch. 709, Stats. 2023) *See* Executive Summary & Comment 2.

AB 1202 (Chau, Ch. 753, Stats. 2019) *See* Comment 2.

****