Articles + Publications | October 19, 2023

California Delete Act: An Aggressive New Approach to Regulating Data Brokers

WRITTEN BY

Ronald Raether, Jr. | Sadia Mirza | Karla Ballesteros | Laura Hamady | Robyn W. Lin

On October 10, Governor Newsom signed the Delete Act (SB 362) into law, which amends California's current data broker law to impose extensive additional disclosure and registration requirements on data brokers, and to require them to support deletion requests through a central "deletion mechanism" developed and administered by the California Privacy Protection Agency (CPPA).

Putting Consumers in the Drivers' Seat

The Delete Act would allow consumers to request deletion of their personal information held by all data brokers registered with a single submission. This effort to shift the burden of preference management from consumers to regulated businesses through a public "deletion mechanism" follows a similar requirement imposed by the California Consumer Privacy Act (CCPA). The CCPA requires businesses to listen for Global Privacy Control (GPC) signals from consumer browsers and treat them as requests to opt out of the sale or sharing of consumer personal information.

Growing Concern Over Data Brokers

The Delete Act may be the latest legislative reaction to a brewing public mistrust of data brokers. Regulatory concern and political commentary about the data broker business in the U.S. is not new. Over the last decade, Congress has been interested in data brokers[1] and the Federal Trade Commission (FTC) has called for greater transparency and accountability from the industry.[2] This interest continues. In April 2023, the U.S. House of Representatives' Energy and Commerce Subcommittee held a hearing to examine the role of data brokers in the digital economy.[3] Though past efforts to pass national legislation have not been successful,[4] concern with the potential consumer harms associated with widespread data collection and sales appears to be gaining momentum.

Federal Agencies and the States Act

In the absence of national regulation, federal agencies and states have started acting independently, adding to the compliance complexity for many businesses.

In 2018, Vermont passed the nation's first broker law, followed in 2019 by California. In 2021 Nevada passed its own law, followed in 2023 by Oregon[5] and Texas[6].

In the fall of 2022, the FTC filed suit against a data broker alleging that it acquired consumers' precise geolocation data and then marketed it in a form that allowed subscribers to track consumers' movements to and from sensitive locations,[7] and in March 2023, the Consumer Financial Protection Bureau (CFPB), launched an inquiry into the business practices of data brokers. The CFPB's inquiry was intended to inform proposed rulemaking under the Fair Credit Reporting Act (FCRA) and was followed in August 2023 with an announcement of the proposed rulemaking. As drafted, the proposed rulemaking could redefine data brokers as consumer reporting agencies (CRA) and classify data held by these companies as a consumer report — subjecting *any entity* that collects and sells consumer data to the FCRA requirements imposed on CRAs.[8] These requirements include reasonable procedures to assure maximum possible accuracy, rights of access and disclosure of "sources," dispute, and investigation requirements. This could also have an upstream effect, turning a data broker's source of personal information into a furnisher. The CFPB's proposed rule is planned to be released for public comment in 2024.[9]

Two Flavors of Data Broker Laws

Notice and Registration. Vermont, Oregon, and Texas all require data brokers to register and provide public notice of their practices but do not require the data brokers to provide any rights or options. For example, as part of the registration process, data brokers in Oregon are required to provide whether Oregon residents may opt out of all or a portion of the data broker's collection, sale, or licensing of personal information.

Notice, Registration, and Providing Consumers with Rights. In Nevada and California, data brokers are required to register in the respective states, provide consumer notice of their practices, and allow consumers with certain individual rights, including the right to opt out of the sale or sharing of consumer personal information.

Definition of "Data Broker"

While current state data broker laws define "data broker" slightly differently[10], all the definitions include the concept of a commercial business that (1) collects personal information about a consumer with whom the business *does not* have a direct relationship, and (2) sells that personal information.[11]

All state data broker laws provide exemptions or thresholds. For example, Texas has a monetary threshold. In Texas, the law only applies to data brokers that derive: (i) more than 50%of their revenue from processing or transferring personal data, or (ii) revenue from processing or transferring the personal data of more than 50,000 individuals, in any 12-month period. Additionally, all state data broker laws except Vermont, exempt activity regulated by the FCRA or activity regulated by the Gramm-Leach-Bliley Act (GLBA).

Penalties and Enforcement. All of the states, except for California, provide a cap for penalties. In Vermont, Oregon, and Texas, penalties may not exceed $10,000, and in Nevada, penalties may not exceed $5,000. California has never provided a cap for penalties. Under California's Delete Act, current fines would increase to $200 each day the data broker fails to (i) register with the CCPA, or (ii) comply with a single deletion request. Penalties can also include (1) unpaid registration fees; and (2) the expenses incurred by the CCPA following an investigation and administration of an action. Because the $200 fine applies to days a data broker fails to register or fails to comply with a single deletion request, this could total to $400 per day.

Significance of California's Expanded Data Broker Law

California's data broker law has always been a bit unique in that it directly imposed CCPA requirements by requiring data brokers to identify how consumers can opt out of sales or submit requests under the CCPA. However, the new requirements will impose greater burdens on data brokers to abide by yet-to-be announced technological requirements, require additional information when registering, and increase penalties and costs.

Expanded Registration Disclosures and Fees. With the Delete Act, data brokers will have to provide more information than was previously required, and the definitions of certain requirements will likely be subject to further rulemaking. Increased requirements will require data brokers to dedicate more time and resources into registering each year. Data brokers will be required to provide information regarding their collection of three highly sensitive data types, specifically:

- Personal information of minors;
- Precise geolocation data; and
- Reproductive health care data.

New Metrics and Annual Disclosures. The Delete Act also imposes new reporting obligations. Data brokers will be required to annually compile and disclose (i) the number of CCPA requests received (ii) the median and mean number of days it took to respond, and (iii) the number of CCPA requests denied, including the reason for the denial. Additionally, data brokers will be required to undergo an audit and maintain records of any compliance audit for at least six years. These new requirements are in addition to the existing required risk assessments and cybersecurity audits imposed by the CCPA.

Participation in a New Technical Mechanism. With the Delete Act, data brokers must take part in the to-be-announced deletion mechanism. While it is unclear what the CPPA will require (the agency has until January 1, 2026, to announce the mechanism), data brokers will have to dedicate time and resources to ensure compliance and are already required to maintain the CCPA's "Do Not Sell or Share" link on their websites in conjunction with their privacy policies. Once announced, data brokers must start using the mechanism by August 1, 2026, and are required to:

- Access it every 45 days.
- Honor deletion requests unless subject to CCPA exceptions.
- Process the request as an opt out of sale or sharing under CCPA, if deletion request is denied.
- Submit to independent audit every three years.

New Regulator. Under the Delete Act, oversight authority over data brokers will be transferred from the attorney

general to the CPPA.

Unintended Consequences

The expanded new requirements are a legal and operational game-changer for organizations that qualify as data brokers. However, there are a few unintended consequences that organizations should consider:

Applicability. As discussed above, the definition of who is a data broker has not changed, however, the risk analysis organizations conduct to make the determination may have. At present, there are only 500 data brokers registered in California, but the current registration likely does not adequately capture the reality of data brokers operating in California. As a result, organizations may face additional scrutiny for failing to register. These companies should act now to conduct an assessment to determine whether they are a data broker, and if not, document the reasons why.

Broader Business Impacts. Compliance with the Delete Act will undoubtedly send a ripple effect to all those organizations that rely on the use of third-party data. Perhaps the most worrisome is that the act may inadvertently undermine safeguards against consumer fraud. For example, many financial institutions and online retailers rely on the data provided by data brokers to verify the identities of their customers, protecting them from fraudulent activities and scammers. Deleting certain personal information, such as past addresses or other historical data, could prevent consumers from accessing their bank accounts or employers from reviewing job applicants.[12]

Technical Complexities. The Delete Act presents two unique challenges for data brokers: verification of requests and a continuing duty of deletion. Under the Delete Act, consumers, or a consumer's "authorized agent," can submit a single deletion request to all registered data brokers. However, data brokers will need to be prepared for the administrative overhead to meet the large volume of requests and proper policies to correctly verify the requests. The Delete Act inadvertently creates a market ripe for exploitation and error. For example, Permission Slip, a mobile application by CR, was created with the sole purpose of assisting consumers with managing their personal information. The application allows a consumer to "send a request to a company to delete their account or stop selling their information" all with a "simple tap." The advent of these mobile applications could result in a large volume of requests for data brokers to process and verify. This challenge is further compounded by continuing obligation of deletion and the nature of data ecosystems. At present, organizations do not have an ongoing obligation to ensure a consumer's data is deleted after complying with an initial request. Under the Delete Act, organizations will be required to check every 45 days to ensure that a consumer's data has been deleted. The ongoing deletion request is further compounded by the fact that not every data broker flags data to associate information with a specific person, and data is constantly changing and being introduced by a variety of sources (*e.g.*, how to determine if new data relates to the person requesting a deletion). As a result, verifying the data across multiple data brokers without a common identifier may prove to be difficult. Thus, organizations may have to take a de facto approach and opt out everyone if it proves too difficult to parse out California residents.

Costs. The Delete Act would authorize the agency to charge a fee to data brokers for accessing the deletion mechanism. However, these costs are not on a sliding scale. The registration fees, the penalties, and the compliance costs are applied equally across all data brokers no matter the size or revenue, which in turn may adversely affect smaller business operations.

Further Guidance to Be Expected

The Delete Act presents a challenge to organizations attempting to understand and comply with the law. The Delete Act leaves many things unclear. In the meantime, organizations will work with legal counsel to ensure appropriate compliance. For example, organizations will need to create internal guidelines for determining who a minor is or what reproductive health care data is in the absence of regulatory guidance.

Key Takeaways

Whether your organization is, or could be, considered a data broker, data obtained or used by your business likely comes from a data broker. Some best practices to assess their applicability and to position your organization to comply with the growing number of data protection laws and regulations in the U.S. include:

1. Conduct data-mapping assessments to understand where your data comes from and where it flows. This will help you understand whether you "sell" or "share" information generally, whether you are potentially a "data broker" under applicable state laws, whether you procure data from data brokers, or may just be required to offer or participate in honoring, certain consumer rights.

2. Determine if you are a data broker and if not, document why.

3. Review registration requirements to ensure timely registration in applicable states.

4. Review webpage to ensure that consumers rights under the CCPA are listed.

5. Maintain deletion request policies accounting for opt-out procedures.

6. Develop and maintain proper internal policies to review deletion requests every 45 days.

7. Develop and maintain record keeping policies reflecting compliance and audit reporting.

8. Conduct employee training and awareness programs to ensure staff members understand and comply with the new regulations.

9. Consider vendor management and contract provisions that contemplate the impact data deletion may have on your business.

---

[1] *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, Government Accountability Office report to the Chairman, Committee on Commerce, Science and Transportation, U.S. Senate (GAO-663), 2013.

[2] *Data Brokers: A Call for Transparency and Accountability,* FTC Report, May 2014.

[3] *Oversight and Investigations Subcommittee Hearing: "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy."* April 19, 2023.

[4] *E.g.*, *Data Broker Accountability and Transparency Act of 2017.*

[5] See Oregon's HB 2052, was signed into law on July 27, 2003 and comes into effect on January 1, 2024.

[6] See Texas' SB 2105

[7] *FTC v. Kochava, Inc.,* August 29, 2022

[8] Consumer Finance Podcast. (2023). "CFPB's Rulemaking Under the FCRA (Part 3) – Crossover Episode With FCRA Focus Podcast" [Audio podcast]. Available at https://www.troutman.com/insights/cfpbs-rulemaking-under-the-fcra-part-3-crossover-episode-with-fcra-focus-podcast.html

[9] Consumerfinance.gov, *Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices,* August 15, 2023.

[10] Importantly for California data brokers, the Delete Act does not change the existing definition of a data broker, which is and has been defined 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." Cal. Civ. Code §1798.99.80(d).

[11] At first glance, Oregon's definition does not appear to have this "direct relationship" requirement, however, the definition of data broker exempts businesses that collect information about a consumer if the consumer is or was a customer, subscriber, or user of the business entity's goods or services. It also exempts other types of "direct relationships", such as if the consumer is an employee of the business. *See* Oregon's HB 2052.

[12] We discuss the consequences of expanding the definition of data broker and imposing certain Fair Information Practice Principles in our Consumer Finance Podcast. (2023). "CFPB's Rulemaking Under the FCRA (Part 3) – Crossover Episode With FCRA Focus Podcast" [Audio podcast]. Available at https://www.troutman.com/insights/cfpbs-rulemaking-under-the-fcra-part-3-crossover-episode-with-fcra-focus-podcast.html.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber