

Insights, News & Events

CALIFORNIA ANNOUNCES GROUNDBREAKING DATA BROKER FINES: 5 STEPS YOUR BUSINESS CAN TAKE TO AVOID BEING NEXT

Insights
Aug 18, 2026

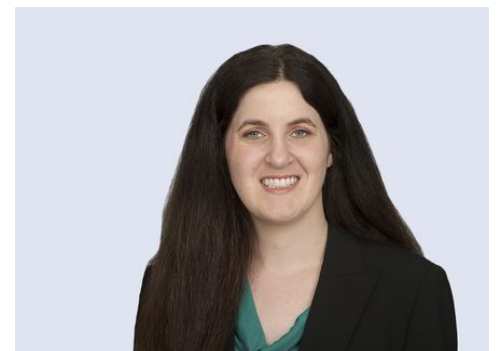
California Announces Groundbreaking Data Broker Fines: 5 Steps Your Business Can Take to Avoid Being Next

California's privacy regulator just fined two companies for mishandling consumer data in actions that should cause any data-handling company to take notice, especially since one settlement expands the way the state pursues enforcement activity. The California Privacy Protection Agency (also known as "CalPrivacy") announced August 10 settlements with Cybba, Inc. and LocateSmarter, LLC, for violations tied to the state's data broker registration law and its broader consumer privacy statute. And while CalPrivacy has brought over a dozen enforcement actions against data brokers before, the settlement with LocateSmarter is the first to combine violations under the California Consumer Privacy Act (CCPA) and the Delete Act into a single action. If your business collects, buys, sells, or licenses consumer data in any capacity, even if you don't identify as a "data broker," these two cases are worth a close look, because you may have more exposure than you think. Here's an overview and a five-step plan you can take.

What Happened?

The two settlements announced last week share some common traits, but they also stand apart from each other in one important respect.

Related People



Darcey M. Groden,
CIPP/US

Partner

858.597.9627



Kile E. Marks, FIP,
CIPP/US, CIPM, CIPT

Associate

LocateSmarter: Data Broker Registration and CCPA Opt-Out Violations

The LocateSmarter order reaches beyond the issue of data broker registration and addresses how businesses should design mechanisms for consumers to exercise CCPA rights.

LocateSmarter provides “data solutions and analytics” services, including location and contact services as well as and fraud-detection products built from personal information it acquires through licensing agreements with other data suppliers. According to CalPrivacy’s factual findings, LocateSmarter’s products disclosed consumers’ names, dates of birth, Social Security numbers, addresses, phone numbers, email addresses, employment information, driver’s license information, military and deceased status, and bankruptcy and litigation history, including inferences about whether a consumer is “litigious.”

The agency found two separate violations:

- **Failure to register under the Delete Act.** Businesses that meet the definition of a “data broker” must register annually with CalPrivacy by January 31 for their data broker activity during the prior calendar year. LocateSmarter did not register by the January 31, 2026, deadline for its 2025 activity.
- **CCPA data minimization violations in the opt-out requests.** LocateSmarter’s online opt-out form required consumers to submit their full name, mailing address, and the last four digits of their Social Security number before it would process a request to opt out of the sale or sharing of their personal information. CalPrivacy had several problems with these practices:
 1. CalPrivacy found this violated the CCPA’s data minimization requirements and its regulations, which bar businesses from treating opt-out requests as “verifiable consumer requests” or otherwise demanding more information than necessary to complete the request. Neither an address nor the last four digits of a Social Security number were necessary to complete the request.
 2. CalPrivacy took particular issue with requiring the last four digits of Social Security numbers because Social Security numbers are sensitive personal information and

858.964.1582



**Xuan Zhou, CIPP/US,
CIPM, CIPP/E**

Associate

858.597.9632

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

the CCPA regulations generally prohibit their usage for identity verification, LocateSmarter had non-sensitive data points it could have used instead, and requiring a Social Security number “could intimidate consumers from exercising their privacy rights.”

3. CalPrivacy noted the predictable result: only a small handful of California’s nearly 40 million residents ever managed to opt out.

Under the settlement, LocateSmarter agreed to pay a \$79,890 administrative fine under the CCPA and a \$30,600 fine under the Delete Act, plus its \$6,000 annual data broker registration fee, totaling \$116,490. LocateSmarter also agreed to register as a data broker going forward, remove the Social Security number and address requirements from its opt-out process, stop requiring verifiable consumer requests for opt-outs, and retrain staff on CCPA compliance.

Cybba: Late Data Broker Registration

Cybba provides “products and services designed for integrated digital marketing of custom audiences.”

According to CalPrivacy’s findings, the personal information Cybba sells includes geolocation data, internet activity data, inferences, identifiers, and commercial data. Its services are intended to reach different behavioral audiences, including business-to-business audiences, purchase audiences, and custom audiences designed to help clients target potential customers. Cybba would assist clients with advertising on social media platforms and building look-a-like audiences.

CalPrivacy’s order determined that Cybba qualified as a data broker because it knowingly collected and sold personal information to third parties concerning consumers with whom it did not have a direct relationship. In addition, Cybba failed to register with CalPrivacy by the January 31, 2025 deadline for its data broker activities during 2024, and did not register until the Enforcement Division contacted it about its failure to register. The company subsequently timely registered in 2026 for its 2025 activities.

Under the stipulated order, Cybba agreed to pay a \$52,400 administrative fine within 30 days. Furthermore, Cybba agreed to timely register in future years in which it operates as a data broker; disclose required metrics concerning CCPA consumer requests in its privacy policy; and access and process deletion requests through the CalPrivacy’s

Delete Request and Opt-out Platform ("DROP") when required.

5 Takeaways for Your Business

What are five steps you should consider taking in order to comply with the law and minimize your exposure?

1. Don't Assume "Data Broker" Status and CCPA

"Business" Status Are Mutually Exclusive. CalPrivacy was explicit that LocateSmarter was both a data broker under the Delete Act and a "business" under the CCPA simultaneously, and that it could pursue violations under both statutes in the same action. If your company sells or licenses consumer data without a direct relationship to the consumer, don't assume Delete Act registration compliance is your only exposure. Your opt-out mechanics, notices, data minimization practices, and broader CCPA compliance program are equally in scope.

2. Don't Treat Opt-Out Requests Like Verification-Required Requests.

California's regulations clearly state that businesses may require a "verifiable consumer request" for the rights to know, delete, or correct, but not for the right to opt out of sale or sharing. Not requiring verification for opt-out requests has been an agency priority since 2024 as well as the subject of ongoing enforcement (see here and here). If your opt-out process asks for anything beyond what's minimally necessary to process the request or includes sensitive identifiers like Social Security numbers (even partial numbers), you may have exposure. You should only request the information necessary to process an opt-out and not create additional verification hurdles that could discourage consumers from exercising their rights.

3. Recognize That Data Minimization Applies to Rights-Request Processes, Not Just Data Collection.

In 2024, CalPrivacy issued an enforcement advisory warning that data minimization applies to rights-request processes, including opting-out of selling/sharing personal information. The LocateSmarter order follows applies the enforcement advisory to a business's actual practices. Before finalizing (or while auditing) your opt-out, deletion, or access request forms, ask whether every field is truly necessary to fulfill that specific request.

4. Eliminate Friction in Your Opt-Out Process.

CalPrivacy pointed to LocateSmarter's low opt-out volume as evidence

the excessive information requirement was working as an obstacle to consumers. It reasoned that the small number of Californians who submitted opt-out requests demonstrated that consumers were intimidated by having to provide sensitive information, including a partial Social Security number. Don't assume that few complaints or low opt-out numbers mean your process is fine. In fact, regulators may view low engagement as a sign the process itself is creating unlawful friction.

5. Mark Your Calendar for January 2027. If your business meets the Delete Act's definition of a data broker for the current calendar year, registration and the registration fee are due between January 1 and January 31 of the following year. Missing that deadline is now demonstrably an independent basis for enforcement under the Delete Act, on top of any separate CCPA violations CalPrivacy may also pursue. These two enforcement actions demonstrate that CalPrivacy is willing to impose monetary penalties when companies that meet the statutory definition of a data broker fail to register on time.

Conclusion

We will continue to monitor CalPrivacy's enforcement activity and provide updates as new decisions are announced, so make sure you are subscribed to [Fisher Phillips's Insight System](#). If you have questions about your organization's CCPA or Delete Act compliance, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our [Privacy and Cyber Practice Group](#).