California Privacy Protection Agency Ramps Up Data Broker Oversight

Aaron J. Burstein, Alexander I. Schneider

March 5, 2025

In recent months, the California Privacy Protection Agency (CPPA) has stepped firmly into a role as the nation's leading data broker regulatory and enforcement agency.

In January, 495 data brokers registered with the CPPA, bringing in an estimated $3.3 million in registration fees.

Last week, the CPPA entered into a settlement with data broker Background Alert, Inc., requiring the company to either suspend its data broker operations for three years or pay a $50,000 fine. The enforcement action marks the seventh case announced by the CPPA since November 2024. The CPPA has the authority to impose a fine of $200 per day that a data broker fails to register. The agency has already settled cases with five data brokers for a total of $226,400 in fines, all for failure to register on time. The CPPA is also pursuing an administrative action against National Public Data to recover a $46,000 fine for failure to register.

Furthermore, on March 6 and 7, the CPPA is slated to consider initiating a new rulemaking regarding data broker deletion obligations pursuant to the DELETE Act. The agency's draft proposed rules would also further refine the definition of a data broker.

Background Alert, Inc. Agrees to Suspend Data Broker Operations for Three Years

According to the Stipulated Final Order, Background Alert failed to register as a data broker by January 31, 2024 despite conducting business as a data broker in 2023. Background Alert, which admitted to the substantive facts in the Order, registered as a data broker on October 8, 2024 after CPPA initiated an investigation, 250 days after the registration deadline. At $200 per day, the applicable fine assessed by CPPA was $50,000.

In lieu of a fine, the parties agreed that Background Alert would cease operations as a data broker for three years, until 2028.

Although Background Alert's data broker product focused on providing access to publicly available information from public records that is not normally considered regulated "personal information" under California privacy law, the CPPA established that Background Alert's processing of inferences *based on* this information constituted personal information. For example, Background Alert allowed users to search for "alarming patterns" or to identify potential family members or associates, which the CPPA alleged are inferences that constitute personal information under the CCPA.

The CPPA explained its concern regarding inferences in the Order: "Inferences present special risks to privacy. Seemingly innocuous data points, when combined with other data points, can be

exploited to infer highly personal characteristics about people. Consumers can be identified, re-identified, and profiled as a result."

The CPPA also pointed to Background Alert's own statements to support the agency's privacy concerns. A testimonial on the company's website stated, "It's scary how much information you can dig up on someone."

CPPA Considers New Rulemaking on Deletion Mechanism

Ahead of its next meeting, the CPPA released draft proposed rules to implement a mechanism for consumers to direct a data broker to delete their data, called the Delete Request and Opt-out Platform (DROP).

Key provisions in the draft proposal include:

- Data brokers would be required to establish an account and pay a first-time access fee of up to $6,600 plus an applicable payment processing fee. (This is in addition to the annual data broker registration fee.)
- Data brokers would be required to access their account at least once every 45 days to access a list of consumers who request that their data be deleted. The initially downloaded list would contain information about all consumers who requested deletion as of that time. Subsequent lists would be limited to consumers who requested deletion after the initial download.
- The draft regulations would require data brokers to match the data they access via DROP with the data in their own records. In particular, the draft regulations require taking steps to increase the likelihood of a positive match, such as removing special characters.
- Where a DROP record includes multiple identifiers, the data broker would be required to compare each identifier with its own records and delete personal information when more than fifty percent of the identifiers match with a particular consumer in the data broker's records. If the data broker does not match any of the identifiers for a consumer in the DROP list, the data broker would be required retain that consumer's DROP record and attempt to find a match in future deletion processes.
- Conversely, if a single identifier matches to multiple consumers, the data broker would be required opt each of those consumers out of the sale or sharing of their personal information.
- Data brokers would not be required to delete first-party data collected directly from the consumer.
- Data brokers would be required to delete inferences about the consumer in addition to other personal information.
- The draft regulations would require a data broker to report how it addressed each request, such as by indicating the record was deleted, not found, or exempted.

Interestingly, the draft regulations would prohibit data brokers from contacting consumers to verify deletion requests submitted through the DROP but also provides consumers "may be required" to verify their California residency with the CPPA before they can submit a deletion request.

The CPPA will consider whether to take action on the draft proposed rules at its next meeting on March 6 and 7, 2025.

CPPA Considers Narrowing Its Expanded Definition of a Data Broker

The DELETE Act 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." As we previously reported on this blog, the CPPA recently modified the definition of a "direct relationship" to potentially exclude some consumer-facing businesses that collect personal information from third-party sources and sell that data to third parties.

Now, the CPPA is considering a rulemaking to further alter what it means to have a "direct relationship." The agency's draft proposal would make the following revisions to the definition of a "direct relationship":

- *Three-year lookback:* The current rule states that a consumer only has a "direct relationship" with a business if the consumer intentionally interacted with the business within the prior three years. The CPPA's latest draft proposal would remove the three-year lookback period.
- *"First party" interaction:* The CPPA clarifies in its draft proposal that a business may be a data broker where it sells personal information collected outside a "first party" interaction with the consumer, defining a "first party" as the business with which the consumer "intends and expects to interact." By incorporating the "first party" concept, the CPPA's draft appears to be clarifying that businesses are *not* data brokers when they process first-party data.

Priorities for Businesses Subject to Registration Requirements

Given CPPA's active enforcement of data broker registration obligations in California, it is important for businesses to determine whether they are data brokers and to register with the CPPA to avoid potential fines for late registration. Registration instructions are available here at the CPPA's website.