

Latest Developments in California Privacy Enforcement in March 2025 – Investigative Sweep and CCPA Enforcement Action

Client Alerts

March 14, 2025

By: Madeleine Findley

California has again made headlines this week with two notable data privacy developments under the California Consumer Privacy Act (“CCPA”): (1) the California Attorney General’s (“California AG”) announcement of a new investigative sweep into the location data industry, and (2) the California Privacy Protection Agency’s (“CPPA”) first public CCPA enforcement action against Honda. In this alert, we highlight the key issues and takeaways from each.

The California Attorney General’s Sweep on Location Data

On March 10, 2025, California AG Rob Bonta announced an ongoing “investigative sweep” into the location data industry. Privacy observers may recall that the California AG has announced similar “investigative sweeps” into CCPA compliance each year since 2022,¹ usually in connection with Data Privacy Day in January. Although this year’s announcement came later, it is taking a broad look at the location data ecosystem. The California AG sent inquiries to advertising networks, mobile app providers, and data brokers seeking information on their collection and processing of “sensitive personal information.” Specifically, the sweep is focused on the fact that precise geolocation data is a form of sensitive personal information under the CCPA, and whether businesses are adequately providing consumers with the right to opt out of the sale or sharing of such information and to request to limit the use of such information.

The California AG’s focus on location data highlights the evolving nature of CCPA enforcement. Previous investigative sweeps have focused on particular industries and their compliance with the CCPA’s right to opt out and other aspects of the CCPA as initially enacted in 2018. This most recent sweep, however, focuses on consumer privacy rights conferred under the California Privacy Rights Act’s (“CPRA”) 2020 revisions to the CCPA. In announcing the sweep, AG Bonta emphasized that location data can reveal other sensitive personal data, noting that location data “can let anyone know if you visit a health clinic or hospital, and can identify your everyday habits and movements.” This reflects the increasing focus in state legislative proposals on enhancing privacy protections for information that can reveal consumers’ habits or movements or information about their health, religious practice, sexuality, or other sensitive data. The sweep extends to the location data

ecosystem broadly. The sweep offers a reminder that businesses that collect and process location data, particularly for advertising purposes, should regularly review their privacy notices, data collection and processing practices, and vendor relationships involving location data for any opportunities to enhance privacy compliance.

The CPPA's First Public CCPA Enforcement Action

In a novel step, on March 12, the CPPA announced its first public CCPA enforcement decision, a settlement and \$632,500 fine against Honda Motor Co. for failing to fully comply with the CCPA. Of that penalty amount, \$382,500 accounts for 153 individual violations of the right to opt-out of the sale or sharing of personal information or to limit the use of sensitive personal information. The settlement arises from the agency's 2023 review of connected vehicle manufacturers and related technologies.

In its order, the CPPA alleges that Honda violated the CCPA by:

- Improperly requiring consumers to verify their identity when submitting requests to opt-out of the sale or sharing of their personal information or to limit use of sensitive personal information and collecting more personal information than necessary;
- Imposing impermissible requirements that consumers directly confirm with the business that they had authorized an agent to submit a request to opt-out of the sale or sharing of their personal information or to limit the use of sensitive personal information, which made such requests more difficult and resulted in overcollection of personal information;
- Requiring consumers to take *two* steps in the company's cookie consent manager when *opting out* of sale or sharing of personal information but only *one* step when *accepting* all cookies or when subsequently opting back in; and
- Failing to produce contracts with advertising technology vendors and thus failing to demonstrate that such contracts contained required terms to protect consumer privacy.

The CPPA also required Honda to confirm in writing to the CPPA within 180 days that it has implemented all required contractual terms with all external recipients of personal information, conducted employee training, and reviewed the user experience for its privacy rights request methods to ensure they are easy to use. In addition, the settlement requires Honda to modify its methods for submitting privacy rights requests; stop requiring consumers to directly confirm that they have given permission to an authorized agent to submit opt-out requests on their behalf; separating opt-out requests and requests to limit from requests that require verification; and applying the Global Privacy Control. In addition, the CPPA ordered Honda to include a "Reject All" button as well as an "Allow All" button in its cookie consent manager, and include a link to manage cookie preferences within its Privacy Center, Privacy Policy, and in its website footer.

As the first public CCPA enforcement from the CPPA, this settlement order offers valuable insight into the agency’s expectations and priorities. Namely, there are three core takeaways from this action against Honda:

- The process for submitting privacy rights requests should be designed to limit requests for additional personal information, except where required (e.g., requests to know, correct, or delete), and should not require identity verification for opt-out requests;
- Cookie consent managers should present symmetrical choices to consumers (e.g., if there is an “Allow All” button, there should also be a “Decline All” button) and businesses should conduct user experience testing to ensure their design is clear and easy to use for consumers; and
- Organizations should have contracts containing relevant privacy terms with all entities that receive personal information, including vendors, service providers, contractors, and third parties.

This settlement reflects the CPPA’s enforcement priorities for 2025. After focusing on data brokers and compliance with the Delete Act in 2024, the CPPA is “prioritizing investigations involving privacy notices, the right to delete, and the implementation of consumer requests,” as well as opt out rights and dark patterns.

Given these latest developments in California’s privacy enforcement and the increasing array of privacy laws and regulations applicable to businesses, we encourage our clients to review their privacy compliance practices. Jenner & Block is prepared to assist with these compliance analyses and advising clients as they navigate this evolving field.

Footnotes

[1] See <https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-puts-businesses-operating-loyalty>; <https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications%E2%80%99%E2%80%99>; <https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance>; <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-investigative-sweep-focuses-streaming-services%E2%80%99%E2%80%99>.

Related Attorneys



Madeleine Findley

Partner

mfindley@jenner.com

+1 202 639 6095

Related Capabilities

Data Privacy and Cybersecurity

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed

