Insights, News & Events

CALIFORNIA SECURES RECORD $12.75 MILLION CCPA SETTLEMENT: YOUR ACTION STEPS TO ENSURE PRIVACY COMPLIANCE

Insights
May 11, 2026

California Secures Record $12.75 Million CCPA Settlement: Your Action Steps to Ensure Privacy Compliance

California officials just announced the largest settlement over alleged violations of the California Consumer Privacy Act (CCPA) to date – a $12.75 million payout. Friday's settlement with General Motors, negotiated by California Attorney General Rob Bonta and several key district attorneys with support from the California Privacy Protection Agency (CalPrivacy), is also the first enforcement action alleging a violation of the CCPA's data minimization requirements. That principle – the idea that you should not collect more data than you need and delete it once the purpose is served – is now an active enforcement priority. The case also targets purpose limitation: once you collect data for a specific reason, you cannot quietly repurpose it later without going back to consumers for consent. If your business collects any kind of consumer or employee data, you should read on to find out what happened, where the regulatory trends are heading, and what you should do to ensure compliance.

What Happened: The Allegations Against GM

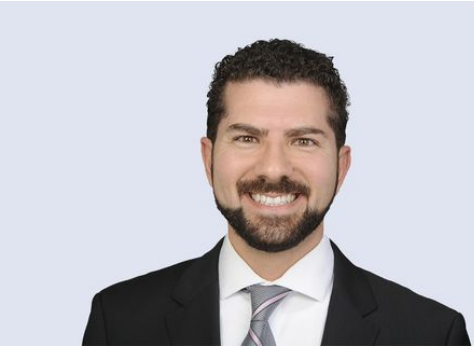
The conduct at issue centers on GM's OnStar program, a vehicle connectivity service that provides roadside assistance and navigation. According to the complaint filed as part of the settlement, GM sold the names, contact information, precise geolocation data, and driving behavior

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627



Usama Kahf, CIPP/US

Partner

data (including speeds, rapid acceleration, and hard braking) of hundreds of thousands of California OnStar subscribers to two data brokers from 2020 to 2024.

The state alleged that GM:

- Sold consumer data without adequate notice or consent, despite telling OnStar subscribers their data would only be used to provide requested services;
- Affirmatively stated in its privacy policy that it did not sell driving or location data; and
- Retained location and driving data long after it was needed for OnStar services and then sold that retained data to brokers, a violation of the CCPA's data minimization requirements.

GM resolved the matter without admitting liability.

The 2 Legal Theories Behind the Settlement

This settlement is built on two distinct legal theories, both of which apply to most businesses.

1. Consent and Disclosure Failures

The CCPA requires businesses to tell consumers what data they collect, how it will be used, and with whom it will be shared – before collecting it. GM's alleged misstep was that it told consumers one thing ("we don't sell your data") and did another (sold it to two data brokers). Moreover, because GM said it did not sell data, it was alleged to have follow-on violations relating to failure to provide notice of selling and the right to opt-out and failure to provide the right to limit the use or disclosure of sensitive personal information (for the alleged disclosure of precise geolocation data). In addition to regulators characterizing this conduct as violating the CCPA, regulators also claimed the allegedly false statements about not selling data violated California's Unfair Competition Law and False Advertising Law.

2. Data Minimization: You Can't Hold Data "Just in Case" or Use Data for Purposes Incompatible with the Original Collection

California's 2023 CCPA amendments require businesses to limit their collection, use, retention, and disclosure of personal information to what is reasonably necessary for the

949.798.2118

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

disclosed purpose. In other words, you cannot collect data for one purpose and then quietly repurpose it later.

In GM's case, the driving and location data was collected to operate OnStar: to summon help, provide directions, and similar functions. Retaining that data indefinitely and then selling it to insurance data brokers was, regulators alleged, a clear violation of the purpose limitation and data minimization rules. Moreover, the data brokers were alleged to have used the data to develop a product for auto insurers that rated drivers based on driving behaviors, despite that such usage-based insurance is illegal in California. In other words, GM's sale of data violated data minimization principles because it was unnecessary – the product be developed was never going to be legally usable by insurers.

For businesses, that means that data you lawfully collect for a specific purpose doesn't become freely available for new business uses down the road. Repurposing retained data, even it was legitimately collected in the first place, requires fresh consumer disclosure and, in many cases, affirmative consent.

Key Questions to Ask

This CCPA enforcement action has broad implications beyond the automotive industry and connected devices; it impacts mobile apps, adtech, employee monitoring platforms, AI analytics tools, wellness technologies, IoT (Internet of Things) ecosystems generally, and more. The settlement is an indication that regulators are now comparing engineering and data flows against public privacy disclosures, reviewing vendor relationships in more detail, and testing whether businesses operationalize their privacy promises.

If you collect any personal information under the CCPA's broad definition (names, contact details, location data, browsing behavior, purchase history, and much more), you should ask the following questions in an internal review:

- Does our privacy policy accurately describe what data we collect and how we use and share it?
- Are we sharing or selling consumer data with third parties? If so, have we provided adequate notice and appropriate CCPA rights (such as the right to opt-out of selling and sharing or the right to limit the use or

disclosure of sensitive personal information, which data sold is sensitive data under the CCPA)?

- Are we retaining data beyond what is needed for its original collection purpose? If you generally collect all data indefinitely regardless of original collection purpose, chances are your answer to this question is no.
- Do our data-sharing agreements with vendors and third parties align with our disclosed privacy practices?
- Are we using data for purposes not compatible with the context in which it was collected? If so, have we obtained consumer consent for such usage?
- Have we assessed our compliance with the CCPA's 2023 data minimization and purpose limitation amendments?

Action Steps for Employers and Businesses

Given the scope and significance of this settlement, we recommend you take the following steps now:

- **Audit your data inventory.** Map what personal information you collect, why you collect it, how long you retain it, and who you share it with.
- **Review and update your privacy policy.** Ensure your consumer-facing disclosures accurately reflect your actual data practices, including any third-party sharing arrangements. Verify that you have accurately and comprehensively described all purposes for which you may use data you collect from or about consumers.
- **Assess data retention and use practices.** Identify whether your business retains personal information beyond the period needed for its disclosed purpose. If so, either delete that data or obtain fresh consent for any new uses that were not previously disclosed to the consumer at the point of collection or that are inconsistent with the consumer's reasonable expectation of what the data would be used for at the point of collection. Implement and operationalize a compliant data retention policy that includes managing and exerting contractual controls over downstream retention by vendors and business partners.
- **Scrutinize third-party data agreements.** Review contracts with data brokers, analytics vendors, advertising platforms, and other third parties that receive consumer

data. Confirm that those arrangements are consistent with your privacy disclosures and the reasonable expectations of consumers.

- **Conduct a privacy risk assessment.** Particularly if your business collects location data, behavioral data, or other sensitive categories of information, a formal privacy risk assessment may be appropriate, and in fact may be required under the CCPA for certain high-risk data uses.

Conclusion

If you have questions about how this settlement affects your organization, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Team or our Consumer Privacy Team. We'll continue to track the latest developments, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.