Insights, News & Events

CALIFORNIA PROBE TARGETS LOCATION DATA INDUSTRY: 5 STEPS TO KEEP YOUR BUSINESS OFF THE CCPA ENFORCEMENT RADAR

Insights
Apr 1, 2025

A new California investigative sweep into the location data industry focuses on whether businesses have violated state law relating to the consumers' right to limit how their personal information – including their geolocation data – is used. This California Consumer Privacy Act (CCPA) enforcement initiative, announced March 10, is part of broader state efforts to crack down on businesses that rely on location tracking. We'll explain what's happening and give you five proactive steps to comply with the CCPA's stringent requirements and avoid getting dinged in the sweep.

Quick Overview

California Attorney General Rob Bonta recently announced an investigative sweep into whether location data businesses (such as advertising networks, mobile app providers, and data brokers) subject to the CCPA offer and implement consumers' right to stop the sale and sharing of personal information, particularly when it is geolocation data. Bonta highlighted growing concerns about the potential misuse of location data, and his March 10 announcement came just days after California lawmakers introduced AB 1355 – a bill that, if passed, would establish strict parameters for employee geolocation tracking technologies.

5-Step Action Plan for California Businesses Subject to the CCPA

1. Conduct a Comprehensive Audit of Website Cookies and Tracking Technologies

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Usama Kahf, CIPP/US

Partner

949.798.2118

Many businesses are unaware of the full scope of tracking technologies embedded in their websites, often underestimating the extent to which these tools collect and share user data. Even if carefully set up, tracking technologies may have data leakage – that is, they may be sending information to third parties without the business's knowledge. Moreover, over time, tracking mechanisms can accumulate from various sources, whether integrated by external vendors or left behind by outdated or forgotten company initiatives. Without comprehensive monitoring and oversight, businesses may unknowingly expose consumer data to third parties, increasing compliance risks under the CCPA and litigation risk under the California Invasion of Privacy Act (CIPA).

To mitigate these risks and maximize compliance, businesses should conduct a comprehensive audit of their website's tracking technologies and consent mechanism (also known as consent management platform or CMP). This process helps to:

- Identify all first- and third-party cookies and tracking mechanisms in use, including those embedded within analytics tools and plug-ins.
- Assess (and test) what information these tools collect, not just what you think they are supposed to be collecting.
- Eliminate any unnecessary or unauthorized tracking technologies that no longer serve a business purpose, reducing the risk of inadvertent data sharing and potential legal exposure.
- Determine proper classification of cookies as essential or non-essential.
- Test whether your CMP is doing what it's supposed to be doing (i.e., that privacy choices users select on a cookie banner actually work).

2. Limit Data Collection to Only What is Necessary

Data minimization – the concept that businesses should only collect data that is strictly necessary and proportionate to accomplish the purposes for which the data is collected – is a fundamental principle underscoring the CCPA. Businesses subject to the CCPA must take a strategic and purpose-driven approach to data collection because indiscriminate

Chelsea Viola
Associate
213.403.9626

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

data collection could increase regulatory and legal exposure and can also erode the trust of clients and customers. To ensure that your business is only collecting what is essential to deliver and provides its products and services, you should:

- ***Tailor data collection to your business model and user demographics.*** Different industries and user bases require different types of data. For example, an e-commerce platform may need shipping addresses, but a purely informational blog post may not require any location tracking at all. Businesses should critically assess whether the data they collect, including geolocation data, aligns with their core functions and target audience.

- ***Exercise heightened caution when handling sensitive personal information.*** In the context of location tracking under the CCPA, sensitive personal information means the location of an individual within approximately 0.38 square miles. Businesses should assess whether the data they collect through cookies falls within this category and determine if there is a clear, legitimate, and legally justifiable reason for doing so. Even when collection is necessary, companies must implement strong safeguards to prevent unauthorized access, misuse, or exploitation.

- ***Think holistically about what a user's interaction with your business can communicate.*** Tracking technologies which can trace people across different websites and build profiles on them may collect a myriad of other sensitive personal information – including health-related information, sexual orientation, immigration status, and religious belief. Businesses need to take a holistic approach to data collection, considering not just the specific data points collected, but whether even disclosure of the fact the user visited your website, app, or specific subparts within it may itself disclose sensitive personal information about the user.

3. Implement a Robust Cookie Management Process

Cookies are small data files stored on a user's device that help websites remember preferences and track browsing history. While some cookies are essential for website functionality, others collect personal data for analytics, marketing, or third-party sharing. Under the CCPA, businesses must provide consumers with clear and

meaningful choices about how their data is being used. To ensure compliance with the CCPA, businesses should:

- ***Implement a user-friendly mechanism for opting out of non-essential cookies.*** This ensures that consumers can easily control their data preferences.
- ***Ensure that cookie consent banners and preference settings comply with regulatory requirements.*** This includes providing clear opt-in and opt-out choices that meet all necessary legal standards. Your website should not require users to take more steps to reject cookies than to accept them (read more about the use of "dark patterns" here).

4. Regularly Test and Audit Your Cookie Compliance Mechanisms

Implementing opt-out mechanisms and consent banners alone is not enough – businesses must actively ensure these tools function correctly and that third-party partners adhere to data privacy obligations. Regular testing and audits help prevent compliance gaps, reduce legal risk, and maintain consumer trust. Businesses should:

- ***Conduct periodic technical audits to verify opt-out functionality***. Regularly test cookie consent tools to ensure consumers can effectively opt out of non-essential cookies and that their preferences are properly honored.
- ***Confirm third-party vendor and advertising partner compliance.*** Review agreements and data-sharing practices to ensure external partners meet contractual and regulatory data privacy obligations. Failure to ensure compliance can expose businesses to legal and financial risks, making it essential to proactively monitor and address any potential issues.
- ***Implement automated monitoring tools to detect unauthorized tracking.*** Use technology to continuously scan for unapproved data collection and third-party scripts that may violate privacy policies or legal requirements. Detecting and addressing these risks proactively helps mitigate any potential noncompliance.

5. If You Receive a Letter From the AG, Don't Panic! Call Your FP privacy Attorney

The Attorney General announced his office will initiate this investigative sweep by sending inquiry letters to advertising networks, mobile app providers, and data brokers and requesting information. Receiving such a letter can be a scary proposition. But don't panic! Our team is ready to help you respond to any such inquiry you may receive. The Fisher Phillips Consumer Privacy Team can help you assess your current state of CCPA compliance and respond to any inquiry in a manner that best protects your business. And if your review of the key takeaways above illustrates you still have some work to do, we can assist with that as well.

Conclusion

The California Attorney General's investigation signals an increasing regulatory focus on location tracking, making it critical for businesses to proactively ensure compliance with the CCPA. Companies must address potential risks posed by outdated tracking technologies, excessive data collection, and inadequate consumer opt-out mechanisms to avoid inadvertent violations. Now is the time to review compliance measures and implement necessary changes.

Fisher Phillips will continue to monitor CCPA obligations and enforcement trends, providing updates as needed. To stay informed, subscribe to Fisher Phillips' Insights System for the latest developments. For further guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Consumer Privacy Team. You can also visit our U.S. Privacy Hub at any time.