Insights, News & Events

CALPRIVACY CONTINUES WEBSITE CRACKDOWN WITH MASSIVE FINES AND OPERATIONAL SUSPENSION: 5 STEPS BUSINESSES SHOULD TAKE

Insights
Nov 23, 2026

CalPrivacy Continues Website Crackdown With Massive Fines and Operational Suspension: 5 Steps Businesses Should Take

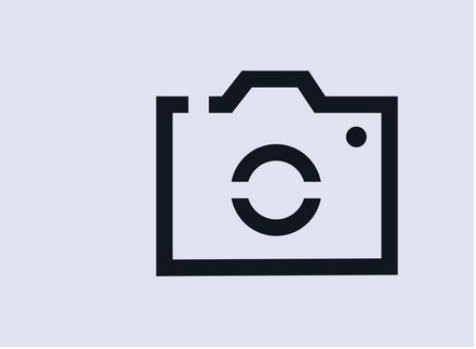
California's privacy regulator just announced two massive fines against businesses whose websites failed to follow privacy compliance standards and sent a warning that other violators might not be allowed to resume business activities until they can demonstrate compliance with state law. The California Privacy Protection Agency (CalPrivacy) announced two decisions on November 17 involving a large car rental agency and a prominent clothing retailer for alleged violations related to processing of opt-out preference signals (OOPS) and sales and sharing of personal information. What stands out are not just the financial penalties – a total of over $1.7M combined – but the message businesses may be required to cease operations until they can verify compliance with audit, testing, and implementation obligations. Here's what you should know and five steps to consider taking.

What Was Wrong With the Websites?

CalPrivacy's November 17 announcement alleged that both businesses failed to configure core aspects of their websites to be compliant with California's privacy laws.

For the car rental agency, CalPrivacy identified three deficient areas of the website:

Related People



Ryan Steidl, CIPP/E
Partner

206.247.7030

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

- *Failure to honor opt-out preference signals.* The business placed several cookies and pixels on its websites. However, it allegedly did not configure its websites to detect and honor opt-out signals such as Global Privacy Control (GPC), which resulted in "selling and sharing" of website visitor data with ad-tech companies and registered data brokers.

- *Failure to include specific information about opt-outs in privacy policies.* CalPrivacy found that the business' notices and disclosures did not provide sufficient information about information practices, available rights, and how to exercise those rights (particularly as it related to out-out preference signals).

- *Failure to properly configure windows for managing cookie preferences.* Although the business did provide a link to "Manage Cookies" that opened a window to select preferences, CalPrivacy found that the interface was misleading and confusing, and that individuals had to take additional and non-obvious steps to actually register their choices.

For the clothing retailer, CalPrivacy identified four deficiencies:

- *Failure to provide required "do not sell or share" link on the website.* Because the business placed tracking technologies on its website and made information available to third parties for advertising purposes, the business was required to post a "Do Not Sell or Share My Personal Information" link or similar opt-out alternative on the website.

- *Failure to provide functional methods for exercising CCPA rights.* Although the business' privacy policy specified privacy rights as required by law, CalPrivacy found that all three methods provided for exercising rights (website link, email, toll-free number) were either broken or non-responsive.

- *Failure to honor opt-out preference signals.* Similar to the car rental agency, CalPrivacy found that the business did not honor opt-out preference signals and consequently continued to sell or share information with ad-tech companies.

San Diego

San Francisco

Silicon Valley

Woodland Hills

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

- *Failure to cease selling or sharing data after consumers opted out.* CalPrivacy additionally detailed the compounding effects from the business' failure to honor opt-outs.

Large Fines + Significant Warnings

CalPrivacy's enforcement included not just impactful fines but stringent administrative obligations to prove compliance.

- For the car rental agency, **a $1.55 million fine** is due within 60 days of the decision's effective date. Additionally, the business must conduct a compliance assessment within six months of the decision, quarterly scans of all websites, and quarterly tests of website configurations and CCPA request methods. It also must maintain an inventory of trackers, establish defined third-party onboarding and management processes, and independently verify consent management functions twice annually. Finally, the business must post CCPA request metrics on its website on an annual basis.

- For the clothing retailer, CalPrivacy imposed **a $217K fine**. It was prepared to seek another multi-million penalty but substantially reduced it after verifying that the business was unable to pay a fine of that magnitude. **The order also requires the business to cease sales and sharing of data to ad-tech companies, and not resume until certifying ability to be compliant**. Other penalties include mandatory quarterly audits to prove the efficacy of processing opt-out preference signals, a requirement to implement and validate adequate mechanisms for exercising rights requests, and conducting company-wide training on CCPA requirements within 30 days of the decision and annually thereafter.

Top 5 Steps to Take Now

You can proactively address the risks and consequences identified from these enforcement actions by considering the following five steps:

1. Understand what information your company shares. Although California has specific requirements related to "sales," many states have requirements relating to sharing, use of data for advertising, and data being processed by data brokers. Conduct an inventory, assessment, or similar step to best understand your data flows.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

2. Implement proper technical components for the form and function of your websites. This can include established requirements such as cookie banners, preference management centers, and recognizing GPCs. It also includes being ready to comply with impending laws (e.g., the California Opt Me Out Act takes effect January 2027, requiring browsers to offer easy-to-use OOPS which automatically communicate privacy preferences to websites).

3. Implement proper legal components for websites. Although California requires specific links and language, all states have requirements for sufficiently detailed notices and privacy policies.

4. Ensure adequate control over outsourced technologies and functions. California and other states have defined requirements for contractual obligations, as well as maintaining oversight over third parties and the data they handle. Have a process in place to evaluate third parties at all phases of the relationship, across due diligence, onboarding, management, and offboarding.

5. Audit regularly (at least once annually). Even if not required by statute, you should routinely review your compliance exposure and posture due to the frequent changes to operations, technologies, and the law. This can help you document and demonstrate defensibility should CalPrivacy, or any other regulator, decide to scrutinize your company.

Conclusion

We will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Practice Group.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.