Insights, News & Events

CALIFORNIA PROPOSAL TO CURB WEBSITE COOKIE LITIGATION STALLS FOR THIS YEAR: WHAT 3 THINGS SHOULD YOUR BUSINESS DO?

Insights
Jul 7, 2025

A California bill aimed at curbing the explosion of lawsuits filed against businesses using common website tools like cookies, pixels, and session replay software has stalled out in the 2025 legislative session, meaning your business will remain vulnerable to the newest type of privacy litigation for at least the next year. Despite the Senate unanimously approving SB 690 just a month ago, the bill's author announced on July 2 that it would be made into a "two-year bill" – meaning it will not advance further this year but may be taken up again in 2026. What does your business need to do to put yourself in the best position to defend against these California Invasion of Privacy Act (CIPA) wiretapping claims?

CIPA's Emergence as a Class Action Weapon

CIPA was originally enacted in 1967 to combat traditional wiretapping and eavesdropping, primarily in the context of telephone communications. It was never designed to address the complexities of the digital age or regulate how businesses track user interactions on the internet.

- However, in recent years, plaintiffs' attorneys have increasingly applied CIPA to modern online contexts, using its language to target routine website technologies such as cookies, pixels, search bar/form, chatbots, and session replay tools.
- These tools are widely used to provide analytics and stats on website traffic, improve website functionality, enhance customer experience, and target ads to website users

Related People

Benjamin M. Ebbink
Partner
916.210.0400

Usama Kahf, CIPP/US
Partner
949.798.2118

when they leave a website in an effort to lure them back to that website.

- Plaintiffs' attorneys, however, argue that these technologies amount to illegal "wiretapping" or the use of "pen registers" and "trap and trace" devices under CIPA, even though they are standard practices across virtually all commercial websites.

Shocking Stats Demonstrate Business Vulnerability

This novel application of a decades-old statute has fueled a dramatic surge in class action lawsuits, catching many businesses off guard and creating a wave of legal risk that CIPA was never intended to address. According to Fisher Phillips' Digital Wiretapping Map, which tracks public filings involving claims tied to digital tracking technologies such as cookies, pixels, and beacons embedded in websites, apps, or marketing emails, there have been 2,341 lawsuits filed nationwide since a landmark court ruling in 2022 opened the door.

Remarkably, 1,845 of these lawsuits – approximately 79% – were filed in California alone. Many businesses are often pressured to settle to avoid the risk of statutory damages and costly litigation, which prompted the introduction of SB 690 to curb these practices.

What SB 690 Was Designed to Do

SB 690 was designed to curb this "shakedown" litigation by clarifying that the wiretapping law should not apply to a business's or its vendors' processing or disclosure of data for a commercial business purpose. It would:

- Exempt activities conducted for commercial business purposes from several core CIPA provisions
- Shield businesses from liability for the interception or recording of communications when done for a commercial business purpose
- Clarify that the use of pen registers and trap and trace devices for commercial purposes is not a CIPA violation
- Eliminate the private right of action for many online tracking claims conducted for commercial business purposes

Chelsea Viola
Associate
213.403.9626

Service Focus

Digital Wiretapping Litigation

Government Relations

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Supporters argued that businesses should not face CIPA liability for conduct already governed and permitted by the California Consumer Privacy Act (CCPA). To resolve this discrepancy, SB 690 proposed aligning the definition of "commercial business purpose" under CIPA with the CCPA. This would have made it clear that routine activities like operational support, security, marketing, and analytics – when performed in accordance with the CCPA – would not violate CIPA.

What Happened?

On July 2, the author of SB 690, State Senator Anna Caballero (D-14), announced she was pausing SB 690, holding it in the Assembly until at least 2026. Caballero cited "outstanding concerns around consumer privacy," and acknowledged continued opposition from consumer privacy advocates and attorneys' groups. This abrupt decision was preceded by its unanimous passage in the Senate just a month earlier, on June 3.

What Should Businesses Do Now?

The withdrawal means that the path to CIPA reform is, at least for now, on pause. Businesses must continue to navigate CIPA litigation without the protections SB 690 would have provided. In the meantime, you should take three proactive steps to protect your business and limit your CIPA exposure while we await any future legal developments that may shift the regulatory landscape.

1. Stay Compliant

Businesses must continue to proactively manage CIPA risk, especially in the absence of immediate legislative reform. Companies should regularly evaluate their practices and ensure they are taking reasonable steps to limit exposure:

- **Review Website Tracking Tools:** Carefully audit all website tracking technologies in use, including cookies, pixels, chatbots, and similar tools. Ensure that these technologies are necessary for your operations and that their use is thoughtfully limited to what is appropriate.
- **Ensure Transparent Consumer Disclosures:** Make sure privacy policies and website disclosures clearly explain how consumer data is collected, used, and shared. Disclosures should specifically address the use of web

tracking technologies and provide users with accessible information about their rights.

- **Assess and Strengthen Consent Practices:** Evaluate whether consumer consent is properly obtained, especially for tracking tools that may trigger heightened scrutiny under CIPA. Consent mechanisms should be clearly presented, easy to understand, and aligned with best practices for affirmative consent where appropriate.

2. Engage in Policy Discussions

Businesses should seize this opportunity to actively engage with trade associations and policymakers to help shape future revisions to SB 690 or other potential CIPA reforms. Now is the time for businesses to have a seat at the table and advocate for practical, balanced privacy legislation that accounts for modern online practices. Ways to get involved include:

- **Lobbying Efforts:** Directly engage with lawmakers and regulatory agencies to communicate the real-world impact of CIPA litigation and emphasize the need for reasonable standards that balance business interests and consumer privacy.
- **Trade Association Participation:** Join and actively contribute to trade groups that are already advocating for CIPA reform on behalf of the business community. These associations often have stronger collective influence and can help drive meaningful policy discussions.
- **Political Engagement:** Participate in public comment periods, attend hearings, and build relationships with key policymakers to ensure businesses are heard as new legislation and amendments are considered.

3. Seek Legal Guidance

Given the fast-evolving nature of CIPA case law, it is critical for businesses to actively partner with legal counsel to manage risk and stay ahead of emerging trends. Fisher Phillips' Digital Wiretapping Litigation Team is uniquely positioned to guide businesses through this complex landscape. Our team closely tracks CIPA developments and has deep experience helping companies mitigate risk and navigate privacy litigation.

Conclusion

To stay informed, subscribe to Fisher Phillips' Insights System for timely updates on CIPA and other privacy-related trends. For personalized guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Digital Wiretapping Litigation Team. You can also explore additional resources on our U.S. Privacy Hub at any time.