

DECEMBER 18, 2025 | PUBLICATION

Client Alert: Website Tracking and Privacy Lawsuits Predicted to Surge in 2026: Practical Steps to Mitigate Risk

Companies operating websites accessible to California residents (essentially all websites) should anticipate continued, and most likely increased, actual and threatened litigation under the California Invasion of Privacy Act (CIPA) in 2026. Anything from an insufficient cookie notice to a website search bar linked to your analytics can give rise to a claim and, with it, \$5,000 in statutory damages per violation. Despite ongoing legislative efforts, no safe harbor currently exists, and businesses remain exposed to significant legal risk.

The most recent attempt by the California legislature, SB 690, did not pass during the 2025 session despite strong support (33-0 in the California Senate). While it is likely to be reintroduced in 2026, it will likely not take effect until January 1, 2027. That gives potential litigants a clear deadline to file all claims they can.

In this environment, proactive risk mitigation through up-to-date privacy and cookie notifications, technical audits and controls, and ensuring that your practices align with your policies is essential.

Background: Surge in CIPA Website-Tracking Claims

CIPA (Cal. Penal Code § 630 et seq.), enacted in the 1960s to address wiretapping and eavesdropping, was later amended to include mobile phones and two-party consent. Since 2020, its application to modern web technologies has increased. Plaintiffs claim tools like pixels, session replay, chat widgets, and search bars intercept or “read” user communications and share data with third parties without valid consent. These claims are attractive to plaintiffs and hard to defend because of CIPA’s statutory damages of \$5,000 per violation, no need for actual damages, inconsistent judicial interpretations, the law’s broad application, and

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne

wbyrne@shumaker.com

issues of consent.

Key Theories in Website-Tracking Litigation

CIPA website-tracking lawsuits typically advance one or more of the following theories:

1. **Wiretapping/Interception Claims (§ 631(a)):** Plaintiffs claim embedded vendor code intercepts private user interactions (keystrokes, clicks, chat messages) that the user has a right to expect to be private unless notified. Vendors are seen as third-party interceptors. Recent court decisions have contributed to uncertainty.
2. **Cell/Telephone-Related Eavesdropping Claims (§ 632.7):** Some complaints attempt to apply provisions originally intended for phone communications to web interactions, often alongside § 631(a) and other claims.
3. **Pen Register/Trap-and-Trace Theories (§§ 638.50–638.51):** A newer litigation trend alleges that certain tracking tools act as pen registers or trap-and-trace devices by capturing routing or signaling information. Courts are divided, and litigation is ongoing.

Legislative Reform: SB 690 and Its Potential Impact

SB 690 aims to reform CIPA's application to website tools commonly used by businesses. The bill passed the California Senate unanimously, stalled in the Assembly, and is now a two-year bill with potential review in 2026. As drafted, SB 690 would:

- Introduce a "commercial business purpose" carve-out, narrowing the scope of CIPA prohibitions for certain data processing activities.
- Define "commercial business purpose" as "the processing of personal information either performed to further a business purpose or subject to a consumer's opt-out rights."
- Limit private rights of action for damages and injunctive relief where personal information is processed for a commercial business purpose.
- Clarify that pen register/trap-and-trace definitions exclude devices or processes used for a commercial business purpose.

Currently, there is no statutory safe harbor, and SB 690 wouldn't provide immediate relief. Critics argue the term "business purpose" may lead to debate and litigation, and CIPA remains a vehicle for claims against website owners. The uncertainty surrounding reform has prompted warnings of increased pre-amendment filings as plaintiffs seek to capitalize on current ambiguities and available damages.

Practical Steps for Risk Mitigation (2025–2026)

Given the evolving legal landscape, companies should adopt a holistic approach to CIPA compliance covering technology, legal, and vendor management. Recommended actions include:

- Inventory and test all third-party cookies, scripts, and SDKs (analytics, pixels, chat, session replay, etc.). Ensure none of your cookies or pixels begin tracking users before they have a chance to decline consent.
- Minimize the data you capture (e.g., by masking form fields, suppressing keystroke capture, and avoiding the collection of sensitive data) wherever possible; however, this approach has proven imperfect in tools such as search bars. When in doubt, disconnect features from third-party tools or analytics rather than relying on your analytics company's artificial intelligence (AI) to detect when someone enters personal information.

- Implement strong consent flows with clear disclosures and opt-out mechanisms *aligned with actual data practices*. If your privacy policy doesn't match your internal practices, you risk a deceptive trade practices lawsuit.
- Update privacy notices (California and others require annual updates) and cookie disclosures to accurately reflect data collection, vendor relationships, and user choices.
- Review your website Terms of Use, particularly regarding communications, chat, and dispute resolution. Ensure user rights are clear, and if you intend to push claims into arbitration or prohibit class actions, use click-wrap agreements.
- Review and strengthen vendor contracts to limit data use to service provision, ban use for vendors' purposes, and require security controls and cooperation on claims.
- Put together a demand-letter response playbook, including technical validation, vendor notification, and settlement strategy.

Key Takeaways

CIPA remains a significant litigation risk for websites transmitting user interactions to vendors in ways that may be characterized as interception or "reading in transit," or put another way, websites that use vendors to operate any aspect of the website, including analytics.

1. Reform efforts have stalled. SB 690, the most prominent proposed reform, will not protect anyone until 2027 and will likely spur additional litigation before any effective date.
2. Alignment among site behavior, consent mechanisms, disclosures, and vendor contracts is critical to reducing legal exposure.

If you would like more information on CIPA website-tracking litigation, SB 690, or how these developments may impact your business, please contact Brian Focht.

Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line is here to provide practical guidance to help you reduce risk and stay ahead of increased website-tracking claims expected in 2026.