

CLIENT ALERT

PRIVACY AND DATA SECURITY

KUTAKROCK
ATTORNEYS AT LAW | KUTAKROCK.COM

November 9, 2026

Services

Privacy and Data Security

Intellectual Property

Technology Transactions and Licensing

Contacts

Larkin Reynolds
Denver
303.297.2400
larkin.reynolds@kutakrock.com

SB 690 Reshapes California Website-Tracking Claims: What Business Leaders Need to Know

For the past few years, large and small businesses alike have faced a flood of privacy lawsuits and demand letters claiming that common website analytics tools constitute illegal "pen registers" under the California Invasion of Privacy Act ("CIPA"). A new California law may change things, but not as much as many had hoped. Specifically, in late September, California Governor Gavin Newsom signed Senate Bill 690 ("SB 690"), which takes away the right of private plaintiffs to sue businesses under the statute. This change matters to companies nationwide: private CIPA suits have targeted businesses all over the country whose websites and apps are visited by Californians. Read on to learn exactly what changed, what risks remain, and what business leaders should do now.

TL; DR:

- California's CIPA was amended. As of January 1, 2027, the statute no longer permits private claims based on the pen register provision of the statute (practically speaking, the provision affecting the collection of data such as IP addresses and device identifiers). The Attorney General can still enforce that provision.
- Claims pending under Section 638.51 commenced on or after January 1, 2025 are also subject to dismissal, assuming this provision survives anticipated litigation challenges.
- The wiretapping and eavesdropping provisions of the law remain unchanged.

Background

CIPA is a 1960s California wiretapping statute that allows recovery of $5,000 per violation, without requiring proof of actual harm. In 2015, California added a "pen register" provision (Penal Code § 638.51), originally aimed at devices that capture phone numbers dialed. To target broad applications of that sort of technology, the law defined "pen register" and "trap and trace device" broadly as any "device or process" that "records or decodes" dialing, routing, addressing, or signaling information without the contents of the communication.

In recent years, plaintiffs' firms have increasingly pointed to the pen register provisions to argue that common website analytics tools (pixels, cookies, analytics scripts), which collect IP addresses or device identifiers, are "pen registers." Plaintiffs have generated a wave of lawsuits, arbitration demands, and demand letters against businesses of all sizes—and including "B2B"-type businesses, which traditionally have not been targeted by consumer privacy-oriented suits. Even companies with little to no business in the state of California have been targeted. Governor Newsom described this trend as the "vexatious use of CIPA lawsuits and demand letters to extract settlements" from small businesses.

Claims That Are Now Harder to Win

Following this change on January 1, 2027, demand letters and claims built solely on a pen register theory lose much of their leverage, because the private plaintiff's remedy for "pen register" (§ 638.51) claims will disappear. However, SB 690 changes only who may bring a claim, but it does not make the underlying conduct lawful.

The Attorney General retains enforcement authority over the collection and sharing of covered categories of information under California law. Interestingly, *pending* private suits are affected too, as actions filed on or after January 1, 2025 are subject to dismissal per the new statute, if the retroactivity provision survives legal challenges.

Claims That Are Still Fair Game

Importantly, many similar claims are untouched by the new law. Plaintiffs' firms are already preparing to re-plead former pen register cases under other statutes, several of which contain the same or similar statutory damages.

- CIPA § 631 (wiretapping): claims that a third-party tool intercepted the "contents" of communications in transit, such as form entries, chat transcripts, or session-replay data.
- CIPA § 632 (eavesdropping): claims of recording confidential communications without all parties' consent.
- Federal Electronic Communications Privacy Act (ECPA) claims, frequently pleaded alongside state wiretap claims.
- Video Privacy Protection Act (VPPA) claims where sites share video-viewing data through pixels without proper consent.
- Fraud and deception theories, where a cookie banner or preference tool allegedly fails to honor a user's rejection of cookies, or drops cookies before obtaining promised consent. Many of these claims have survived motions to dismiss.
- Common-law privacy and unfair or deceptive practices claims, plus other statutory claims.

What Businesses Should Do Now

The substantive limits of California's law have not changed. For that reason, companies can still move forward on plans to stay in line by conducting careful audits of what fires on page load and identifying which vendors receive data.

- Test, but don't remove your cookie banner. Confirm that a "reject" or "block" function actually blocks trackers and that your banner says only what your site actually does; mismatches fuel deception claims.
- Revisit pending matters and demand letters. If you face a § 638.51 claim filed on or after January 1, 2025, discuss SB 690 with your counsel and reassess available arguments.
- Use this moment to focus on general privacy housekeeping: Update your privacy notice. Describe tracking technologies, third-party recipients, and opt-out rights accurately, including honoring universal opt-out signals required under various state laws.
- Assess vendor data use and contract protections. Require analytics and advertising vendors to limit data use, support consent controls, and provide indemnification for failures where possible.
- Build a privacy focus into your diligence readiness. Investors and acquirers increasingly ask about tracking practices and open privacy claims; clean records support smoother financings and exits.

Kutak Rock's attorneys are available to counsel you so you can protect your business from potential liability under CIPA. Please reach out to the firm's privacy and data security group if you have questions or need assistance.

This Client Alert is a publication of Kutak Rock LLP. This publication is intended to notify our clients and friends of current events and provide general information about privacy and data security. This Client Alert is not intended, nor should it be used, as specific legal advice, and it does not create an attorney-client relationship. This communication could be considered advertising in some jurisdictions. The choice of a lawyer is an important decision and should not be based solely upon advertisements.

©Kutak Rock LLP 2026 – All Rights Reserved