

Publications

October 1, 2026 • Updates

One Claim Down, Many Risks Remain: What SB 690 Means for Web Tracking Litigation

Key Takeaway

- California Governor Gavin Newsom signed Senate Bill 690 into law, limiting private enforcement of certain California Invasion of Privacy Act (CIPA) claims. Once the law takes effect on Jan. 1, 2027, only the California Attorney General may bring an action under “pen register” and “trap-and-trace” claims against entities based on conduct occurring on websites and online or mobile applications.

Why It Matters

- The relief is meaningful but narrow. SB 690 does not establish a general safe harbor for cookies, pixels, session-replay tools, chat technologies or other online tracking tools. It also does not repeal CIPA’s wiretapping and confidential-communication provisions, which remain available to private plaintiffs.

Next Steps

- Businesses should continue assessing their online data flows, consent mechanisms, opt-in and opt-out configurations and vendor relationships. Website tracking activity can support claims under other provisions of CIPA, the federal Electronic Communications Privacy Act, state wiretapping and consumer-protection statutes and common-law theories.

California Governor Gavin Newsom has signed SB 690 into law, narrowing one avenue used in recent lawsuits and demand letters alleging that ordinary website and application technologies operate as unlawful “pen registers” or “trap-and-trace” devices under Section 638.51 of the California Penal Code.

Once it becomes effective on Jan. 1, 2027, the law will amend Penal Code Section 637.2 to provide that only the California Attorney General may bring an action under that section against a company for a Section 638.1 violation alleging conduct occurring on websites, online applications or mobile applications. The amendment also applies retroactively to pending claims in actions commenced within two years before the law’s operative date.

Related People

- Starr Turner Drum
- Tyler G.D. Anders
- Xeris E. Gregory

Related Capabilities

- Privacy & Cybersecurity

For companies facing claims only under Section 638.1, the relief is significant. But businesses should not interpret SB 690 as resolving the broader litigation risk associated with online tracking. The law changes one private enforcement mechanism, but it does not repeal Section 638.51 or prevent plaintiffs from pursuing other claims based on the same underlying technologies.

What SB 690 Changes — and What It Does Not

Section 638.51 generally prohibits a person from installing or using a pen register or trap-and-trace device without first obtaining a court order. The statute contains exceptions for certain electronic or wire communications service providers, including where the provider has obtained the user's consent.

Separately, CIPA's civil remedies provision currently authorizes private plaintiffs to seek the greater of \$5,000 per violation or three times their actual damages, and it does not require proof of actual damages as a prerequisite to suit. As a result, claims involving digital technologies can create substantial exposure even where a plaintiff does not allege a measurable financial loss.

Plaintiffs have attempted to apply these provisions to website and application technologies that collect or transmit information such as internet protocol addresses, device identifiers, URLs and browsing events. Their theory is that the technologies collect information identifying the source or destination of electronic communications and therefore qualify as pen registers or trap-and-trace devices.

SB 690 creates an express exception to CIPA's private civil-remedies provision. For a Section 638.51 violation alleged to arise from conduct occurring on a website, online application or mobile application, an action under Section 637.2 against a private actor may be brought only by the Attorney General.

The law also provides that this limitation applies retroactively to any pending claim in an action commenced within two years before SB 690's operative date. Defendants facing Section 638.51 claims therefore may have a basis to seek dismissal of those claims. The retroactivity provision may also generate litigation over its application to particular pending actions and procedural postures.

The benefit for businesses is real, but the law's limits are equally important:

- SB 690 does not repeal Section 638.51 or declare website tracking technologies lawful.
- It changes who may bring a covered civil action under Section 637.2; it does not eliminate the Attorney General's authority.
- It applies only to actions against private actors arising from conduct on websites and online or mobile applications.
- Most importantly, it does not amend CIPA Sections 631 or 632 or restrict private plaintiffs from seeking statutory damages for alleged violations of those provisions.

Businesses involved in pending litigation should therefore analyze each complaint claim by claim. Dismissal of a Section 638.51 count may materially reduce a case, but it may not dispose of wiretapping, recording, contract, consumer-protection or common-law claims arising from the same technology.

Web Tracking Litigation Risk Remains

CIPA Section 631 generally prohibits willfully and without the consent of all parties reading or attempting to learn the contents or meaning of a communication while it is in transit. It

also expressly addresses parties that aid, employ or conspire with another person to engage in prohibited conduct. Section 632 separately addresses the intentional eavesdropping upon or recording of a confidential communication without the consent of all parties. SB 690 leaves both provisions unchanged.

These provisions remain potential vehicles for claims involving session-replay software, advertising pixels, chat tools, form analytics and other third-party code. Whether a particular deployment constitutes an interception, captures the “contents” of a communication, involves a third-party eavesdropper, occurs while a communication is in transit or is supported by effective consent will often depend on technical implementation and the allegations pleaded.

Nor are plaintiffs limited to CIPA. Depending on the website, data and users involved, tracking-related allegations may also be brought under:

- The federal Electronic Communications Privacy Act, which authorizes a private civil action and provides for \$10,000, punitive damages, attorneys’ fees and equitable relief for intentional interception of electronic communications;
- State constitutional and common-law privacy theories, including intrusion upon seclusion;
- Breach-of-contract or implied-contract theories based on privacy notices, consent banners or other public representations; and
- State unfair or deceptive practices statutes.

The threshold question for businesses therefore is not whether SB 690 forecloses a private pen-register claim. Rather, businesses should understand what information each technology collects, when it begins collecting that information, where it transmits the information, whether it reveals or is linked to sensitive activity, what the recipient may do with it and whether the company’s consent and opt-out mechanisms operate as represented.

What Businesses Should Do Now

Organizations that operate websites, mobile applications or authenticated portals should consider:

- **Inventorying online technologies.** Identify advertising pixels, analytics tools, session-replay software, chat services, customer-experience platforms, software development kits and other code capable of observing or transmitting user activity. Include technologies introduced through tag managers, plug-ins and downstream vendor integrations.
- **Mapping actual data transmissions.** Determine the specific data elements transmitted to each recipient, including page URLs, query strings, form-field values, search terms, chat content, account identifiers, device identifiers and event metadata. A vendor’s product description or contractual label may not reflect the tool’s actual configuration.
- **Testing the timing and effectiveness of consent.** Confirm whether technologies activate before a user makes a choice, whether the consent language describes the relevant collection and disclosures, and whether rejecting optional technologies actually prevents them from loading. Maintain evidence of the language, configuration and user experience in effect during each relevant period.
- **Reviewing vendor roles and contracts.** Contracts should address permitted uses, required privacy terms, configuration changes, audit rights, data retention, deletion, cooperation and allocation of litigation risk.
- **Implementing ongoing change management.** Tracking risk is not resolved through

a one-time scan. New campaigns, tags, application releases and vendor updates can change data flows without corresponding updates to privacy notices, consent tools or contractual documentation.

- **Reassessing pending demands and litigation.** Companies facing Section 638.51 claims should evaluate whether SB 690's provisions may apply, while preserving defenses to any remaining CIPA or non-CIPA claims.

SB 690 closes an important route plaintiffs use to challenge website and application technologies. It does not, however, close the broader web tracking litigation landscape. Businesses that treat the bill as a comprehensive safe harbor risk overlooking the statutory, contractual and technical issues likely to shape the next generation of claims.

Polsinelli's Technology Transactions & Data Privacy team continues to monitor the implementation of SB 690 and developments in web tracking litigation. Please reach out to our team for further guidance.