California Narrows CIPA Website Tracking Suits: What SB 690 Does and Doesn't Change

By Christopher E. Hart and Martell Johnson

As we have written previously, having a website means being a privacy litigation target. For the past several years, businesses that run websites and apps available to California consumers have faced a steady stream of lawsuits and demand letters under the California Invasion of Privacy Act (CIPA), an all-party consent wiretap statute enacted in 1967 to address telephone interception practices.

Despite being enacted decades before the World Wide Web was a glimmer in anyone's eye, the law is attractive to privacy plaintiffs for three reasons: first, it provides for statutory damages (that is, you need not show actual harm); second, it affects anyone with a website (so long as California residents use it); and third, it ostensibly requires express consent, making it more likely to catch organizations that have less than foolproof operational controls. Despite various litigation successes by defendants, CIPA has become a consistent and ubiquitous source of litigation risk.

To reduce some of this litigation risk, on September 30, 2026, California Governor Gavin Newsom signed Senate Bill 690, eliminating a private right of action for one of the most commonly asserted CIPA theories. This will provide relief for businesses, but understanding the law's limits will help shape risk mitigation efforts.

What the CIPA Amendment Does

SB 690 amends a single CIPA provision: Penal Code Section 637.2, CIPA's enforcement provision, as it relates to Section 638.51, the so-called "pen register" or "trap and trace" provision. Section 637.2 allows anyone injured by a violation of the chapter to sue for the greater of $5,000 per violation or three times actual damages, as well as to seek an injunction. While plaintiffs may show actual damages, they are not required to do so.

The amendment removes the private right of action for online pen register claims. It adds a new subdivision (d) to Section 637.2, which provides that a civil action for a violation of Section 638.51—so long as the violation is alleged to arise from conduct on an internet website, online application, or mobile application—may be brought only by the Attorney General.

Who It Affects

Understanding who SB 690 affects requires understanding how the pen register theory differs from CIPA's more familiar wiretap theory. A wiretap claim under Section 631 targets the **contents** of a communication—what a visitor types into a chat window, search bar, or form—and alleges that a third party read or recorded those contents in transit without all parties' consent.

A pen register claim under Section 638.51, by contrast, does not depend on contents at all. CIPA defines a pen register as a device or process that records or decodes "dialing, routing, addressing, or signaling information." That definition, borrowed from the federal pen register statute and added to CIPA in 2015, was written with recordings of numbers dialed from a telephone line in mind. Plaintiffs have argued that common third-party tools, such as analytics scripts and advertising pixels that capture a visitor's IP address, device, and browser information, are modern-day pen registers.

Because the pen register theory reaches routing and addressing data that nearly every website collects, it has been easier to plead than a wiretap claim and has swept in a far broader range of businesses—including small businesses that, as the Governor noted, may install tracking software without fully appreciating how it tracks or shares visitor information.

SB 690 eliminates private suits only on the pen register theory, and only for online conduct; enforcement of Section 638.51 against websites and apps now rests solely with the Attorney General. Wiretap claims based on the contents of communications, however, remain fully available to private plaintiffs.

When It Becomes Effective

The law goes into effect on January 1, 2027. The amendment is retroactive and applies to any pending claim in an action filed within two years before the bill's effective date. As such, qualifying online pen register claims in private suits filed on or after roughly January 1, 2025, and still pending, would fall within the new limitation. This retroactive application may be challenged; plaintiffs could argue, for example, that eliminating accrued claims raises due process concerns. Defendants in cases subject to the retroactivity provision should consult with counsel to determine appropriate actions, including moving to dismiss.

Why It Matters—and Why CIPA Litigation Isn't Going Away

Pen register claims became a staple of website privacy litigation in part because courts never reached a consensus on them. Some courts accepted that tracking software capturing IP addresses and similar data could qualify as a "pen register" under CIPA's broad definition, while others rejected the theory, reasoning that a statute aimed at telephone surveillance should not be stretched to cover routine website analytics. That inconsistency, combined with exposure to $5,000 in statutory damages per violation, created strong pressure to settle. By routing online Section 638.51 enforcement exclusively through the Attorney General, SB 690 removes that leverage for this category of claims.

But SB 690 is not going to end CIPA litigation. Absent a comprehensive amendment to the law, plaintiffs will continue to be creative. The Governor himself acknowledged that "additional work in this area is needed, as CIPA contains other decades-old statutes that are also susceptible to abuse by overly aggressive litigants." Recent demand letters we have seen already account for the new limitation; businesses should expect plaintiffs to shift toward the theories that remain available—including, for example, claims that voice AI tools used in customer service calls and virtual assistants record or analyze conversations in violation of CIPA's wiretap and eavesdropping provisions.

What It Does Not Change

SB 690 affects only one CIPA theory, and eliminates only the private right of action. A more comprehensive fix was considered but (for now) rejected: an earlier draft of SB 690 would have exempted any "commercial business purpose" from CIPA's wiretapping (Section 631), eavesdropping (Section 632), and cellular interception (Section 632.7) provisions. It would also have excluded such uses from the definitions of "pen register" and "trap and trace device" and from the private right of action altogether. The Legislature removed all of those provisions in favor of a much narrower reform.

As a result:

- **Wiretapping and eavesdropping claims remain available.** Private plaintiffs may still sue under Section 631, which underlies most website privacy suits involving session replay, chat features, and pixels, and under Sections 632 and 632.7, which underlie call-recording and voice AI claims.
- **Section 638.51 itself is unchanged.** Using a pen register or trap and trace device is still prohibited under the text of the statute, absent a court order or a statutory exception (including the consent of the user), and the Attorney General may enforce that ban against online conduct.
- **Pen register claims that do not involve websites or apps are unaffected.** The new limitation applies only to claims arising from conduct on websites, online applications, and mobile applications. A private plaintiff may still bring a Section 638.51 claim based on other conduct, such as tracking outgoing or incoming call

information on a traditional telephone line.

- **Claims against public actors are unaffected.** The limitation applies to actions against "a private actor."
- **Statutory damages remain.** The $5,000-per-violation remedy and the no-actual-damages rule still apply to every private claim CIPA continues to permit.
- **There is no CCPA-compliance defense.** The proposed "commercial business purpose" exemption tied to the California Consumer Privacy Act did not survive, so complying with the CCPA does not by itself shield a business from CIPA liability.

The Bottom Line

SB 690 is a meaningful amendment to a heavily litigated CIPA theory, offering potential relief in pending cases—for now. It does not end CIPA website tracking litigation. Businesses will need to continue evaluating litigation risks stemming from website tracking technologies and, increasingly, AI technologies, which may be fodder for new claims.

This post is for general informational purposes only and does not constitute legal advice.