Now & Next

Cybersecurity & Privacy Alert

September 3, 2026

California legislature passes SB 690: What the bill means for businesses facing CIPA litigation

By Stacy Boven and Lauren Kim

The California legislature passed Senate Bill 690 (SB 690), which would bar individual plaintiffs from bringing pen register and trap and trace claims under the California Invasion of Privacy Act (CIPA). If enacted, SB 690 would significantly reduce CIPA litigation, but it will not end website tracking claims in California. Understanding what SB 690 changes—and what risks remain—is essential.

What's the impact?

- SB 690 would bar *private actors* from asserting CIPA pen register and trap and trace claims related to websites, apps, and mobile apps.
- The bill will shift enforcement to the California attorney general and apply retroactively.
- SB 690 is narrow—wiretapping, Comprehensive Computer Data Access and Fraud Act (CDAFA), unfair competition, and other related privacy claims may still proceed.

SB 690's key provisions

SB 690 amends California Penal Code Section 637.2, the provision that authorizes private parties to sue under CIPA. In short, if enacted, the bill:

- **Bars private actors from filing suit.** Individuals and class-action plaintiffs could no longer sue a private company for pen register or trap and trace violations tied to activity on a website, online application, or mobile app.
- **Gives enforcement to the attorney general.** The attorney general would retain exclusive authority to bring these specific claims.
- **Applies retroactively.** Critically, the limitation would extend to pending claims filed within two years before the bill's operative date, meaning it could impact litigation that has already been threatened or filed.

SB 690's limitations and anticipated impact

SB 690 is considerably narrower than many businesses anticipated. Earlier drafts of SB 690 proposed amendments to Sections 631, 632, 632.7, and 638.50 and a sweeping "commercial business purpose" exemption to CIPA's most heavily litigated provisions. None of those provisions made it into the final bill. Equally important, SB 690 does not make the underlying conduct legal. It merely removes a private plaintiff's ability to bring a Section 638.51 pen register or trap and trace claim and hands that enforcement authority to the attorney general.

Accordingly, SB 690 represents a meaningful win for businesses defending against CIPA pen register and trap and trace claims, but companies should not treat it as the end of their CIPA or website tracking exposure because:

- **Federal and other state claims are untouched**. The bill changes California law only. For example, individual plaintiffs may still assert claims under the federal Electronic Communications Privacy Act (ECPA) or other state law equivalents.
- **The private right of action for other CIPA theories survives**. The bill covers only pen register and trap and trace claims. Wiretapping and eavesdropping claims under CIPA Sections 631, 632, and 632.7—often aimed at pixels, chatbots, and session-replay tools—are unaffected.
- **Other claims persist**. Common law invasion of privacy, CDAFA, California Consumer Privacy Act claims, and unfair-competition theories remain unchanged.
- **Underlying conduct is not deemed legal.** The attorney general can still assert pen register and trap and trace claims under CIPA.

The bottom line: SB 690 changes who can sue for CIPA pen register or trap and trace claims, not what companies are allowed to do. Companies should expect plaintiffs to pivot to other state and federal wiretapping and common law theories. Consequently, certain defenses will remain significant, including those built on consent, the party exemption (and its crime-tort exception for ECPA claims), insufficient "contents of a communication," and non-contemporaneous interception.

What's next

SB 690 is not yet law. The bill now goes to the governor, who must sign the bill into law for it to take effect. Because the bill contains no urgency clause, if the governor signs it during the 2026 legislative session, it will likely take effect on January 1, 2027. The bill would apply retroactively to "any pending claim in an action commenced within two years before the operative date of that legislation," so businesses should take note of the operative date to determine which pending claims may fall within SB 690's reach.

What businesses should do now

Because SB 690 is narrow in scope, still awaits the governor's signature, and could face a constitutional challenge over its retroactivity, businesses with public-facing websites should keep taking proactive steps to mitigate their litigation risk, including working with legal counsel to:

- Monitor the enactment and judicial treatment of SB 690.
- Ensure website and app terms of use, cookie policies, and privacy disclosures are accurate, current, and compliant with all applicable privacy regulations; consider building in additional contractual protections where appropriate.
- Align data practices, cookie banners, and other consent tools with business priorities and litigation risk tolerance—eliminating unnecessary data collection/sharing and obtaining prior user consent whenever possible.
- Address pending or new litigation threats and demand letters promptly by assessing what risk remains and preparing to efficiently defend those claims.

Nixon Peabody's Cybersecurity & Privacy team helps businesses assess and reduce website tracking risks, respond to CIPA, ECPA, CDAFA, and related litigation, and build practical data governance programs. We continue to monitor SB 690 and can help clients prepare for its impact.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Stacy Boven
415.984.8312
sboven@nixonpeabody.com

Lauren Kim
213.629.6158
lkim@nixonpeabody.com