What To Know About Bill Aiming To Curb CIPA

By **Katherine Alphonso and Avazeh Pourhamzeh** (July 14, 2025)

Katherine Alphonso

Avazeh Pourhamzeh

The California Invasion of Privacy Act is a series of statutes intended to prevent unauthorized surveillance and recording of communications in California.

The law was originally passed to avert wiretapping and eavesdropping on phone calls without the consent of all participants,[1] but has recently expanded to include website tracking technologies such as session replays, tracking pixels, chat interfaces, beacons and third-party cookies — tools that are not only common, but integral to digital operations.

In recent years, CIPA-based lawsuits have surged, with plaintiffs attorneys using CIPA as a catchall statute to target website analytics and other digital marketing technologies, including when a company records its own website data — or contracts with a vendor to do so — for the purpose of understanding user behavior for more targeted engagements and/or advertising.

While some of these cases raise legitimate privacy concerns, many have the hallmarks of abusive litigation, including forum shopping, demand letters backed by the threat of ruinous discovery, and lawsuits targeting companies for industry standard practices that consumers largely expect. In addition, these cases often stretch the definitions of key terms, such as "interception" and "wiretapping," applying criminal surveillance standards to ordinary commercial conduct.

The result: a flood of class actions, many seeking damages in the millions based on statutory damages of $5,000 per violation[2] — despite the absence of actual harm, deception or unauthorized disclosure.

Indeed, when courts apply inconsistent legal principles, it creates a patchwork of rulings. For example, in January, in Sanchez v. Cars.com Inc., the Los Angeles County Superior Court held that website tracking technologies did not constitute pen registers or track-and-trace devices used to record or decode dialing, routing, addressing or signaling information from telephone numbers, and therefore are not within CIPA.[3]

For another example from January, in Rodriguez v. Autotrader.com Inc., the U.S. District Court for the Central District of California held that CIPA plausibly covered the tracking software at issue, because the defendant did not explain why the additionally collected information was necessary to operate its website.[4] Nonetheless, even with conflicting lower court decisions, CIPA claims based on website tracking technologies have proceeded past the motion to dismiss or demurrer stage of litigation.[5]

On Feb. 24, Sen. Anna M. Caballero, D-Salinas, introduced S.B. 690, which amends CIPA to allow for the use of website tracking technologies, provided they are used for a commercial business purpose and comply with existing laws like the California Consumer Privacy Act.[6] On June 3, the California Senate passed S.B. 690 with a unanimous vote. The bill has now moved to the California State Assembly where it's been referred to the Committee on

Privacy and Consumer Protection.

For businesses, particularly those operating in California's tech-heavy economy, S.B. 690 is a legal necessity. This carveout for companies that engage in data collection for a commercial business purpose, as defined under the CCPA, narrows CIPA's reach to its intended scope — actual surreptitious recordings or interceptions by unauthorized third parties.

In other words, it recalibrates CIPA by limiting its scope to truly invasive or unauthorized data collection. Not only does this help preserve CIPA's original function as a tool to deter egregious privacy violations, but it also avoids the risk of courts or future legislatures striking down or significantly weakening the statute in response to its misuse.

Litigation Legitimized: How S.B. 690 Strengthens the Future of Privacy Claims

At first glance, S.B. 690 appears to undermine plaintiffs' rights by narrowing access to California's expansive privacy laws — CIPA's penalties are higher than the CCPA's, and the CCPA generally does not provide a private right of action for the same or similar claims as CIPA.[7] But a closer inspection suggests the bill has more pros than cons, including:

- Protecting businesses from abusive litigation;
- Providing much-needed clarity for both plaintiffs and defendants alike;
- Reining in the emerging trend under CIPA of strict liability for ordinary commercial conduct;
- Arguably forestalling drastic responses — preemption arguments, constitutional challenges or legislative repeal — that could erode antisurveillance laws altogether;
- Moving California privacy toward a more sustainable enforcement model. For plaintiffs, that might mean fewer cases in the short term, but stronger and more meritorious ones in the long term;
- Allowing cases to receive meaningful attention and support from the courts as plaintiffs bring claims for practices that are actionable under CIPA, allowing them to focus on genuine privacy violations rather than highly speculative allegations; and
- Encouraging businesses to put forth clearer notices, as well as better consent mechanisms for protecting consumer privacy.

In a legal environment increasingly wary of perceived overreach and opportunistic lawsuits, S.B. 690 filters out low-merit lawsuits, clarifies statutory thresholds, and ultimately gives greater weight and credibility to claims that allege genuine unauthorized surveillance.

Legislating Influence: How S.B. 690 Could Reshape Privacy Law Across the U.S.

In the absence of federal privacy legislation, individual states must step up to shape the future of privacy protections and digital accountability in the U.S. California's move to modernize its antiquated wiretap statute and redraw the line on what counts as actionable surveillance through S.B. 690 could redefine not only consumer protections in-state, but also influence how courts and legislatures across the country balance privacy rights against

the practical demands of modern commerce.

After all, what passes in Sacramento often becomes the legislative template for other states. After California passed the landmark CCPA in 2018, for example, more than a dozen states, including Virginia, Colorado and Connecticut, enacted their own versions of privacy legislation.

If S.B. 690 becomes law, it too could trigger a wave of similar bills across the country, especially in states that have seen rising litigation over website tracking technologies under outdated eavesdropping laws.

Notably, states like Pennsylvania, Florida, Illinois and Massachusetts all have similar wiretap statutes that plaintiff firms have repurposed to target companies using website tracking technologies.

If California can successfully reform its laws to stem abusive litigation while preserving consumer transparency and protection, business advocates in other states are almost certain to lobby for parallel reforms.

Conclusion: S.B. 690 Ensures Meaningful Privacy Enforcement

S.B. 690 serves as a vital piece of legislation that strengthens protections — not just for plaintiffs, but defendants too — by bringing clarity on which website tracking technologies are not actionable under CIPA. It curbs and discourages abusive litigation against defendants and makes it easier for plaintiffs to understand their rights and pursue claims with confidence.

In addition, S.B. 690 in effect encourages businesses to adopt clearer data practices and more robust consent mechanisms, not only empowering consumers, but also strengthening the foundation for meaningful privacy protections.

Katherine Alphonso is of counsel and Avazeh Pourhamzeh is a law clerk at Kaufman Dolowich LLP.

[1] Cal. Penal Code § 630; see Kight v. CashCall, Inc., 200 Cal.App.4th 1377, 1392 (2011) (stating "[t]he Legislature enacted section 632 to ensure an individual's right to control the firsthand dissemination of a confidential communication, and expressed its intent to strongly protect an individual's privacy rights in electronic communications.").

[2] Cal. Penal Code § 637.2(a).

[3] Sanchez v. Cars.com, 2025 WL 487194, at *3 (Cal. Super. Ct. Jan. 27, 2025).

[4] Rodriguez v. Autotrader.com, Inc., 762 F.Supp.3d 921, 929-30 (C.D. Cal. Jan. 8, 2025).

[5] See Esparza v. Kohl's, Inc. 723 F.Supp.3d 934, 943-44 (S.D. Cal. Mar. 18,

2024); Ambriz v. Google, LLC, 2025 WL 830450, at *2-6 (N.D. Cal. Feb. 10, 2025); Greenley v. Kochava, Inc., 684 F.Supp.3d 1024, 1050-51 (S.D. Cal. July 27, 2023).

[6] Cal. S.B. 690, 2025-2026 Reg. Sess. (2025).

[7] See Cal. Civ. Code §§ 1798.150, 1798.199.90(a); Cal. Penal Code §§ 632(a), 637.2(a).