

Title: CIPA Reform Gives Companies a Carve-Out but No Cure: Plaintiffs Pivot as SB 690 Is Signed into Law

Brief Overview: Following a groundswell of lobbying efforts by individual businesses, trade associations and chambers of commerce, Senate Bill 690 was finally passed in both the California State Assembly and Senate in 2026.

In its final form, SB 690 eliminates the private right of action under the California Invasion of Privacy Act (CIPA) for violations of the pen register and trap-and-trace portion of that statute.

On September 30, 2026, Governor Gavin Newsom signed SB 690 into law.

Learn more about SB 690, including takeaways for companies concerning website privacy claims and how to prepare for 2027.

Authors:

[Jennifer M. Oliver](#)

[619 685 1990](#)

Full Article: More than three years into the avalanche of lawsuits against website owners alleging that use of commonplace advertising, analytics, and other “tracking” pixels constitute a violation of various privacy laws, website owners saw a glimmer of hope.

Following a groundswell of lobbying efforts by individual businesses, trade associations and chambers of commerce, Senate Bill 690 was finally passed in both the California State Assembly and Senate in 2026. In its final form, SB 690 eliminates the private right of action under the California Invasion of Privacy Act (CIPA) for violations of the pen register and trap-and-trace portion of that statute. On September 30, 2026, Governor Gavin Newsom signed SB 690 into law.

Effective January 1, 2027, SB 690 will restrict civil enforcement for violations of CIPA § 638.51 (which addresses pen register and trap and trace device use on internet apps and websites) such that only the California Attorney General’s office will have standing to bring civil actions for violations of § 638.51 regarding internet-based conduct. SB 690 is retroactive and applies to pending claims filed on or after January 1, 2025, but does not affect demands or non-pending claims.

Governor Newsom’s letter to the members of the Senate addressed CIPA lawsuits explicitly, and also included a call to action to the Legislature to continue their work to reform CIPA by amending other sections of that law that were not amended by SB 690 and are often leveraged against small businesses in nuisance lawsuits:



OFFICE OF THE GOVERNOR

SEP 30 2026

To the Members of the California State Senate:

I am signing Senate Bill 690, which eliminates the private right of action under the California Invasion of Privacy Act (CIPA) for violations of the pen register and trap-and-trace statute arising from conduct occurring on an internet website, online application, or mobile application.

This measure addresses the vexatious use of CIPA lawsuits and demand letters to extract settlement money from small businesses that unwittingly install software on their websites that at times have tracked and shared the information of visitors to the site. I applaud the author's efforts and align myself with the goal of protecting small businesses from overzealous lawsuits based on a statute written without today's complex technological landscape in mind. However, additional work in this area is needed, as CIPA contains other decades-old statutes that are also susceptible to abuse by overly aggressive litigants. I urge the Legislature to take this on next year to ensure a fair balance between protecting private information and preventing rapacious litigation.

Sincerely,



Gavin Newsom

This is good news for website owners, of course; the amended law significantly narrows the scope of private litigation. But claims under CIPA's wiretapping section § 631 (wiretapping) remain unaffected. And even if the Legislature does eventually amend CIPA to carve out § 631 claims in this context, other statutes such as the Electronic Communications Privacy Act (ECPA) and California Comprehensive Data Access and Fraud Act (CDAFA) are also available tools for plaintiffs.

In fact, seeing change on the horizon, plaintiffs¹ began to pivot toward these alternative theories of liability months ago. Claims under CDAFA, codified at California Penal Code § 502, are on the rise. Plaintiffs alleging violation of CDAFA typically allege that by installing third-party scripts that collect information about website users, the company is “knowingly access[ing] and without permission tak[ing]...data from a computer” in violation of Cal. Penal Code § 502(c)(2) or “knowingly and without permission...caus[ing] to be accessed any computer” in violation of Cal. Penal Code § 502(c)(7), or that the tracking technology is a “computer contaminant” “knowingly introduce[d] [to] a computer.” At least at the motion to dismiss stage, some courts have allowed these claims to proceed. And unlike CIPA, CDAFA has an attorney's fees provision, making it especially appealing to prospective plaintiffs and their attorneys.

Claims under the federal Electronic Communications Privacy Act (ECPA) are also the rise. For years, plaintiffs rarely leveraged the ECPA because it contains a safe harbor provision if one party to a communication consents to its interception. In other words, if the website owner consents to the tracking, there is no violation.

However, the ECPA also contains a “crime-tort exception”: if the violation occurs in furtherance of an underlying criminal or tortious objective, then the safe harbor does not

apply. Plaintiffs first tested the boundaries of the crime-tort exception in the healthcare industry, arguing that tracking on those defendants' websites constitutes an underlying criminal or tortious violation of HIPAA. At least some courts agreed. Plaintiffs then tested the exception even further, arguing that if a defendant's own privacy policy or consent banner misstates its tracking practices, then the plaintiff can state a common law claim for intrusion or invasion of privacy, and the crime-tort exception should apply. Again, at least one court agreed.

The takeaway here is simple: progress is being made on the legislative side, but website tracking lawsuits continue to evolve and persist. The only way to protect your business from these claims is to implement a compliant consent banner and conduct regular, diligent audits of tracking technologies and privacy policies.

Buchanan's [Cybersecurity and Data Privacy](#) team is available to answer questions about how these developments affect your organization. Please contact the author or any member of our team at cyber@bipc.com.

1. Prolific law firms and tester plaintiffs in CIPA cases include Pacific Trial Attorneys, Jarrett Charo, Manning Law APC, Swigart Law Group, Beverly Hills Trial Attorneys, The Law Offices of Jibrael S. Hindi, Gutride Safier, Yao Mou, Vivek Shah, Miltita Casillas, Silvia Garcia, Arisha Byars, Jose Licea, Anne Heiting, Monica Sanchez, Miguel Esparza, Rebeka Rodriguez, Marielita Palacios, Annette Cody, Jerry Aviles, Sonya Valenzuela, Gabriela Hernandez, Sonya Valenzuela, Elizabeth Haviland, Courtney Mitchener, Nora Guterrez, Lillian Jurdi, Dana Hughes, Courtney Mitchener, Ramy Eden, Sheila Biglang-AWA-Castro, Michael Sandoval, Joseph Sides, Apex Trial Attorneys, Heriberto Valliente, Srinivas Rangam, Seyed Hosseini, Bryson Harris, Levi & Korsinsky, Leeds Brown, Dwoskin Wasdin, Zermay Law, Tauler Smith, T.K.C. Lanagan, and Stephanie St. Paul.