

California Turns Down the Heat on Online Tracking Litigation – Congress Introduces Federal Bill to Put Out the Fire

By Matthew H. Meade, Elizabeth Wilson and Roger LaLonde

Current Business Risk

Businesses of all sizes and in all industries are dealing with thousands¹ of demand letters and lawsuits alleging violations of state and federal wiretapping laws (in particular the California Invasion of Privacy Act² (CIPA)) for embedding third-party online tracking tools (e.g., cookies, pixels, and/or session replay software) on their websites, mobile apps, and other online services. Disagreement among courts on how to apply these wiretapping laws which often predate the internet to online tracking tools further fanned the flames of settlement demands and litigation. With businesses facing possible statutory damages of up to \$10,000 per violation, as well as potential punitive damages and attorney's fees, addressing a demand letter or lawsuit can be quite costly.³

CIPA Amendment Enacted to Reduce California Wiretapping Lawsuits

Fortunately for businesses, California's Governor Gavin Newsom signed SB 690 into law on September 30, 2026.⁴ SB-690 amends the CIPA to prohibit private parties from filing suit against a defendant under that law's pen register and trap and trace provisions, to the extent the alleged violation arises from the use of tracking tools on websites, app, and other online services. The amendment will take effect on January 1, 2027, and will apply "retroactively to any pending claim in an action commenced within two years before" that date. This prohibition does not apply to other sections of the CIPA, though, some of which Governor Newsom notes "are also susceptible to abuse by overly aggressive litigants."⁵ This amendment will also not affect claims under the federal Electronic Communications Privacy Act ("ECPA") or other states' wiretapping laws. Businesses with active litigation or demand letters should assess the extent to which this amendment can help them in dismissing, settling, or resolving their respective CIPA claims.

¹ See: Chairman Williams Op-Ed: Stop the Wiretap Shakedown on Main Street (September 28, 2026), available at: <https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=407500> ("Attorneys have filed more than 5,600 lawsuits alleging that common website tools — including chat boxes, cookies, analytics software, and pixels — violate the decades-old wiretapping law.").

² California Penal Code §§ 630-638.55, available at:

https://leginfo.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&part=1.&title=15.&chapter=1.5.

³ For example, the CIPA includes statutory damages of up to \$5,000 *per violation* or up to three times the amount of actual damages suffered by the Plaintiff, whichever is greater. The federal wiretap statute, the Electronic Communications Privacy Act (ECPA), includes statutory damages of up to \$10,000 per violation or \$100 per day, whichever is greater.

⁴ See: https://leginfo.ca.gov/faces/billHistoryClient.xhtml?bill_id=202520260SB690 and <https://www.gov.ca.gov/wp-content/uploads/2026/09/SIGN-msg-SB-690.pdf>.

⁵ See <https://www.gov.ca.gov/wp-content/uploads/2026/09/SIGN-msg-SB-690.pdf>.

Potential Relief from Congress

On September 3, 2026, Congress also got into the fray by introducing H.R. 10263 - Halt Abusive Internet Lawsuits Act of 2026⁶ to address abusive lawsuits alleging violations under the ECPA and other state wiretap laws. The bill prohibits claims or enforcement actions under federal and state wiretap laws for businesses who collect and share information or communications for a “commercial purpose” and included in the definition of “commercial purpose” is data sharing for marketing and advertising purposes, among other common business operations.⁷ This new federal legislation further states that claims or enforcement actions in progress as of the date of the law’s enactment “may not be maintained, adjudicated, or arbitrated after such date.” The bill is still in early stages, and it is unclear whether it will pass, but businesses should continue to monitor the bill’s progress.

Conclusion

While these legislative efforts are providing some relief to businesses, the risk of pixel and other online tracking lawsuits remains. Businesses should consider doing the following to help avoid becoming a target for demand letters and lawsuits under wiretapping laws:

- **Inspect Your Website Tools.** Conduct an audit of your website tools (e.g., cookies, pixels, session replay software, and chatbots) to see what is embedded on your website, what categories of data are shared with third parties through these tools (e.g., advertisers, social media platforms, and data analytics companies), and why the information is being shared. Get rid of any tools you no longer need.
- **Review Your Online Disclosures.** Review your privacy policy, terms of use, and other online documentation to ensure you accurately and comprehensively disclose your data collection and sharing activities.
- **Implement a Cookie Consent Mechanism.** A defense to wiretapping lawsuits is consumer consent. Implement a cookie consent banner that fully discloses and obtains enforceable consent for your website tracking activities, in addition to any opt-outs that can be used to reject tracking. **You must ensure that no tracking occurs until after consumer consent is obtained and implement a procedure to regularly test your consent mechanism to ensure it is working properly.**
- **Review Your Third-Party Contracts.** If you are sharing data with third parties, review and update your third-party agreements, when possible, to include data use restrictions and data protection provisions.

How We Can Help



This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact [Matthew H. Meade](mailto:mmeade@eckertseamans.com) at 412.566.6983 or mmeade@eckertseamans.com, [Elizabeth Wilson](mailto:ewilson@eckertseamans.com) at 215.851.8497 or ewilson@eckertseamans.com, [Roger LaLonde](mailto:rlalonde@eckertseamans.com) at 215.851.8503 or rlalonde@eckertseamans.com, any other attorney in our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

⁶ See: <https://www.congress.gov/bill/119th-congress/house-bill/10263/text>

⁷ See Sections 2(a)(1) and 2(b)(1) of H.R. 10263 (“The collection, processing, or disclosure of information or communications for a commercial purpose shall give rise to no claim or enforcement action under Federal or State law with respect to pen registers, wiretapping, trap and trace, or eavesdropping, including chapter 1.5 of the Penal Code of California”).