ECKERT SEAMANS
ATTORNEYS AT LAW

September 2025

Cybersecurity, Data Protection & Privacy Update

WARNING! IF YOUR WEBSITE USES THIRD-PARTY PIXELS OR TRACKING TECHNOLOGY YOU COULD BECOME A LITIGATION TARGET

By Matthew H. Meade, Elizabeth Wilson & Roger LaLonde

A recent wave[1] of class action lawsuits alleging that website operators violate the California Invasion of Privacy Act (CIPA)[2] when they use third-party online tracking tools (e.g., cookies, pixels, and/or session replay software) should be cause for concern for website operators. Courts are currently split on how to apply the CIPA to website tracking pending an expected amendment to the law, thereby providing a window of opportunity to capitalize on uncertainty with a flurry of demand letters and court filings in the hopes of a quick settlement. With potential statutory damages of up to $5,000 *per violation* or up to three times the amount of actual damages suffered by the Plaintiff, as well as potential punitive damages and attorney's fees, businesses may face threats of significant monetary damages. Therefore, organizations should employ certain measures on their website to reduce the risk of being a target for these lawsuits.

What is the CIPA?

The CIPA is a criminal statute that was first enacted in 1967 to prohibit phone or telegraph wiretapping. Since the CIPA is broadly worded to cover the use of any "device or process," though, Plaintiff's firms are trying to apply this law to third-party tracking tools on websites that collect IP addresses or other arguably identifiable information to monitor users' online behavior. The following arguments are being used as a basis for CIPA claims against website operators.

- *Defendant's Website Tracking Tool is a Trap and Trace Device or Pen Register*. The plaintiff may argue that the defendant violated Section 638.51 of the CIPA by installing a website tracking tool, to the extent such tool could be a "pen register"3 or a "trap and trace device."4 Traditionally, pen registers are devices that record phone numbers dialed by a particular phone (i.e., they capture outgoing information) and trap and trace devices record phone numbers that call a particular phone (i.e., they capture incoming information). Plaintiffs may argue that the data collected by an online tracking tool (e.g., device information or website activity) qualifies as a trap and trace device or pen register.
- *Aiding and Abetting Third-Party Wiretapping:* Plaintiffs may also argue that a defendant violated Section 631(a) of the CIPA by aiding and abetting a third party to unlawfully wiretap communications

[1] As of August 27, 2025, 1,500 CIPA lawsuits have been filed in the last 18 months. *See* Adam J. Brody, Jeffrey M. Stefan II, Neil E. Youngdahl, CALIFORNIA BILL AIMS TO LIMIT COOKIE PRIVACY LAWSUITS, NAT'L LAW REV., August 27, 2025, *available at:* https://natlawreview.com/article/california-bill-aims-limit-cookie-privacy-lawsuits.

[2] California Penal Code §§ 630-638.55, available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&part=1.&title=15.&chapter=1.5

[3] A pen register is defined as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." *See* California Penal Code § 638.50(b).

[4] A trap and trace device is defined as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *See* California Penal Code Section § 638.50(c).

without the plaintiff's consent.[5] Plaintiffs may claim that the use of an online tracking tool allows a third party (e.g., Google, Meta, or other social media providers) to intercept their communications. This legal theory is typically used when a website operator uses a third-party chat bot that captures a web user's communications or installs session replay software to capture a web user's device information and activity on the website (e.g., mouse clicks and keystrokes) in real time.

- *Other Miscellaneous Complaints:* Plaintiffs also may tack on other miscellaneous claims including violations of the California Constitution, the California Data Access and Fraud Act, and/or invasion of privacy claims under California common law.

What Can I Do to Avoid Being A Target For These Lawsuits?

Organizations should employ the following actions below to decrease their likelihood of receiving a CIPA lawsuit.

- *Audit Your Website.* Website operators should evaluate the types of online tracking tools they employ to collect user website activity and/or communications including cookies and tracking pixels, session replay software, and chatbots. Website operators should consult with their third-party website developer, client relationship, and/or marketing service providers to ensure that all online tracking tools are identified and reviewed. Any tracking tools that are not needed or used should be removed from the website immediately.
- *Assess Website Data Collection and Disclosure Practices.* Website operators should then analyze (i) what data is being collected from website tracking tools, (ii) who is receiving this data, and (iii) how the organization and third-party recipients are using the data.
- *Review / Revise Website Disclosures.* Next, website operators should review and, if necessary, update any website disclosures (i.e., privacy policies and/or consents) based on the results of their analyses to ensure that their website collection and tracking activities are fully disclosed to website users.
- *Adopt a Cookie Consent Mechanism.* Lastly, website operators may reduce their risk of being a target for CIPA claims by employing sufficiently detailed and transparent cookie consent mechanisms on their website. When implementing a cookie consent banner, website operators must ensure that the cookie consent language clearly articulates the types of online tracking employed and the purposes for such tracking. Additionally, the consent mechanism must provide real choice to the website user and not engage in "dark patterns," which refer to mechanisms that manipulate or influence a website user's choices, or that make it harder for a user to exercise such choices.

Potential Relief on the Horizon

On June 3, 2025, the California Senate unanimously passed Senate Bill 690[6], which would amend the CIPA to specify that pen registers and trap and trace devices do not include any device or process that is used in a manner consistent with a "commercial business purpose" subject to any opt out rights that may be available to the individual. If the bill passes, the use of website tracking tools for a commercial business purpose will not be considered a violation of the CIPA. Last month, the California Assembly voted to advance the bill, however it will

[5] An entity can violate Section 631(a) by engaging in or aiding and abetting a third party to engage in one of the following: (i) intentional wiretapping; (ii) willfully attempting to learn the contents or meaning of a communication in transit; or (iii) attempting to use or communicate information obtained as a result of engaging in either of the previous two activities. *See Gershzon v. Meta Platforms, Inc.*, No. 23-cv-00083-SI, 2023 WL 5420234 at *11-12 (N.D. Cal. Aug. 22, 2023) (citing *Tavernetti v. Super. Ct. of San Diego Cnty.*, 22 Cal.3d 187, 192, 148 Cal.Rptr. 883, 583 P.2d 737 (1978)) (denying motion to dismiss CIPA claim asserted against use of a Meta pixel).

[6] *See* https://legiscan.com/CA/rollcall/SB690/id/1577634.

not be addressed until 2026. In the meantime, website operators should employ the actions described above to reduce their chance of receiving a demand letter or lawsuit.

How We Can Help.

ECKERT SEAMANS ATTORNEYS AT LAW

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 at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, Roger LaLonde at 215.851.8503 or rlalonde@eckertseamans.com, a member of 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.