Morrison Cohen

**Client Alert** | April 21, 2026

# Website Data Collection and User Interaction Technologies Under CIPA: Key Risks for Businesses

If your company operates a website that California residents can access, you may face exposure under California's Invasion of Privacy Act, Cal. Penal Code §§ 630 et seq. ("CIPA"). A growing wave of private lawsuits and arbitration claims are seeking to apply CIPA to ordinary website technologies, including analytics tools, advertising pixels, session replay software, and live chat features, often without any allegation of actual harm.

## 1. What Is Happening

CIPA was originally enacted in 1967 to target and outlaw eavesdropping, telephone wiretapping and nonconsensual recording. The statute allows individual plaintiffs to sue violators and collect statutory damages. Over the years, the statute has expanded to encompass new technologies. These expansions are sometimes through statutory amendment and other times through new litigation approaches developed by claimants intended to extend the statute's reach.

While plaintiffs and their attorneys have brought various claims under CIPA against website operators, more recently, these claims include the assertion that website operators are violating the statute by using third-party tools, such as Google Analytics, a Meta Pixel, a Hotjar session recording tool, a Salesforce chat widget or similar technologies on their sites. The claimants argue that these tools automatically capture and transmit technical information about a visitor's browser or device and are therefore considered "pen registers" under Section 638.51. The statute bars use of "pen registers" absent consent or court order.

Whether or not these tools are "pen registers" under CIPA has not been definitively settled by the courts and may depend on certain factual and legal nuances. However, several recent decisions by U.S. district courts in California have denied motions to dismiss complaints that alleged use of certain web technologies are unlawful "pen registers" in violation of CIPA. The statute defines a "pen register" broadly as a device or process that records dialing, routing, addressing, or signaling information transmitted in connection with an electronic communication. These claims remain highly fact specific. Risk often turns on how the technology is configured, what information it captures, when it is triggered, and whether the user has been given a meaningful opportunity to consent before the tool begins collecting data. Still, the volume of recent claims makes clear that companies should not assume that commonly used website technologies present little legal risk simply because they are widely deployed.

## 2. Why This May Apply to You

A company does not need to be based in California to face a CIPA claim. The statute is being invoked on behalf of California residents, and plaintiffs generally allege that the relevant tracking technology is installed or activated when the California resident visits the site. As a result, businesses headquartered outside California may face exposure if California residents access their websites and third-party tools begin operating before meaningful consent is obtained.

In practical terms, that means a retailer based in Texas, a SaaS company headquartered in New York, or a healthcare provider operating in Florida could all receive a CIPA demand if their websites are accessible to California residents and use third-party technologies in a manner that plaintiffs contend violates the statute.

## 3. How These Cases Are Brought

The current wave of litigation appears to be driven both by specialized plaintiffs' firms and by individual plaintiffs proceeding without counsel. In many cases, the complaints follow familiar patterns and target similar categories of website technologies under similar liability theories.

Companies typically receive a written demand – often before any lawsuit or consumer arbitration claim is filed – sometimes accompanied by screenshots, code snippets, or other technical material that document the alleged violation. In many instances, engaging counsel promptly upon receipt of a demand letter places the company in a stronger position than waiting until the claim has been formally filed.

A number of plaintiffs' firms and individual plaintiffs have filed or threatened to file such suits based on Section 638.51 and/or other CIPA provisions. Certain law firms and pro se claimants are known to frequently assert these CIPA claims and have brought literally dozens of these claims phrased nearly identically against websites of all kinds with varying amounts of web traffic.

## 4. Key Areas to Consider

Companies that have not recently evaluated their website practices for compliance with current law may wish to consider the following questions.

- Does your site have a cookie banner and consent request that appear immediately upon accessing the site? At what point in the page load sequence do your third-party tools begin executing as compared with when any consent notice is displayed to the user?
- What does your privacy policy say about third-party data collection, and is it specific enough to put a reasonable user on notice of the tools you use?
- Do you maintain a current inventory of every third-party script, pixel, SDK, and tag active on your website, and do you understand what data each transmits and to whom?
- If your site includes a live chat tool, chatbot, or similar interactive feature, how is that feature presented to users, and what information does it collect before or during the interaction?

There is no single way to design and operate a website and it will depend on the company's technology stack, business model, and risk tolerance. Nevertheless, considering and evaluating the responses to these questions are essential for assessing and mitigating risk from aggressive plaintiffs.

## 5. How Morrison Cohen Can Help

Morrison Cohen has extensive experience assisting clients who have received demands alleging CIPA violations, including multiple experiences dealing with repeat plaintiffs' firms and pro se plaintiffs. Our Technology, Data & IP team regularly advises clients on proactive maintenance and best practices relating to CIPA and other privacy laws and defends against CIPA claims when brought. If you have received a demand letter or are facing a filed complaint or arbitration claim, we can help you assess the relevant legal and factual issues quickly, evaluate potential defenses, and determine the most efficient strategic path forward both for the claim and your website. If you have not yet received a demand but would like to better understand your potential exposure and/or how we can work with your team to review your website practices and identify areas where adjustments may reduce risk, please feel free to contact the attorneys listed below.

## Key Contacts

If you require additional information regarding website data collection and user interaction technologies under CIPA, please feel free to contact our Technology, Data & IP attorneys listed below.

**Fred H. Perkins**
*Partner & Co-Chair*

D 212.735.8647
fhperkins@morrisoncohen.com

**Alvin C. Lin**
*Partner*

D 212.735.8873
alin@morrisoncohen.com

**Cesar Rodriguez**
*Associate*

D 212.735.8867
crodriguez@morrisoncohen.com