Tucker Ellis LLP

The CIPA Demand Letter Tsunami: What You Need to Know and What You Can Do About It

JULY 2026

By Alexander R. Safyan and Roylance (Lance) L. Bird

If your business has received a website privacy demand letter from Vivek Shah or a plaintiffs' class action firm, you are far from alone. Thousands of businesses nationwide—including manufacturers, retailers, service providers, technology companies, and many others with no obvious connection to California—have received these letters since Fall 2025. The letters generally follow the same script: they allege that your website's use of cookies, pixels, or other analytics tools violates the California Invasion of Privacy Act (CIPA), a nearly 60-year-old wiretapping law that private plaintiffs have recently begun using to assert website privacy claims. They threaten statutory damages of up to $5,000 per violation, creating potential exposure that can quickly reach six or even seven figures depending on how each website interaction is counted.

Tucker Ellis has already represented more than a dozen clients who have received these demands. This alert explains what is driving the recent wave of claims, what to do if your business receives a demand, and what steps you can take to reduce the risk of becoming a target.

What Is CIPA and Why Does It Matter Now?

California enacted CIPA in 1967 as an anti-eavesdropping and wiretapping statute aimed at telephone communications. In the last few years, however, plaintiffs—most notably Vivek Shah—and plaintiffs' attorneys have sought to apply its provisions to modern website tracking technologies the law was never designed to regulate.

The key statutory provisions are:

- Section 631(a), which prohibits the intentional interception or reading of the contents of communications while they are in transit without the consent of all parties.
- Sections 638.50 and 638.51, which define and restrict the use of "pen registers" or "trap and trace devices" (devices that record routing, addressing, or signaling information for outgoing and incoming communications).
- Section 637.2, which creates a private right of action allowing the greater of $5,000 per violation or three times the plaintiff's actual damages, as well as injunctive relief.

Plaintiffs now contend that ordinary website tools, such as Google Analytics, Meta Pixel, chat tools, and session replay programs, violate these provisions when they transmit information about a visitor's activity to a third party before the visitor provides consent. Their theory is that when these tools capture information such as search terms, clicks, URLs, or IP addresses and transmit it to vendors like Google or Meta, there has been an unlawful interception of the visitor's communication or use of a prohibited pen register or trap and trace device. Because plaintiffs often attempt to characterize each visit, transmission, or third-party recipient as a separate violation, the claimed statutory damages can escalate rapidly, even when the technology was installed for routine business purposes.

These claims have fueled a wave of lawsuits, arbitration demands, and pre-suit letters, forcing businesses to confront substantial potential liability and defense costs under legal theories that remain unsettled. The risk is not limited to California-based companies: an out-of-state business may still face a claim if the visitor is a California resident or alleges that the challenged interaction occurred while the visitor was in California. Any business with a publicly accessible website reachable by users in California may therefore be exposed, regardless of the company's physical location.

The Fractured State of the Law

California courts are sharply divided over whether CIPA's wiretapping and pen register provisions apply to modern website tracking technologies. Some courts have treated cookies, pixels, and similar website tools as potentially falling within CIPA's broad statutory language, particularly where data is transmitted before the visitor has an opportunity to consent. Others have taken a narrower view, concluding that ordinary website functions do not amount to unlawful interception or the use of a pen register or trap and trace device, and that CIPA should not be extended beyond the telephone-focused context in which its provisions were enacted. The disagreement extends to what qualifies as an "interception," whether the website operator is a party to the communication, whether the collection of IP addresses or device identifiers is sufficient, and whether a privacy policy or cookie banner provides effective consent. Courts have also reached varying results on threshold issues such as standing and personal jurisdiction, meaning that substantially similar claims may survive in one courtroom and be dismissed in another.

The result is a patchwork of inconsistent trial court rulings that leaves businesses without clear guidance on how CIPA applies to their websites. But the California Courts of Appeal may soon provide some clarity. In two currently pending cases, *Variety Media, LLC v. Superior Court* and *Reuters News & Media, Inc. v. Superior Court*, the courts are considering whether CIPA's pen register prohibition extends to routine website technologies that collect IP addresses, device identifiers, browser information, and similar data. *Variety Media* also

presents more fundamental questions about whether loading a webpage constitutes an underlying "communication" within the meaning of the statute and whether cookies that collect device-level data record information associated with such a communication. Either case could produce the first published California appellate decision directly addressing whether CIPA applies to routine website technology and substantially reshape the litigation landscape.

Two Major Developments

Two recent developments may also begin to curb some of the litigation. On July 20, 2026, a federal court in the Central District of California issued an order declaring Vivek Shah a vexatious litigant, finding that his pattern of filing similar CIPA actions and dismissing them when challenged strongly indicated an effort to pressure defendants into settlements rather than pursue the claims in good faith. The pre-filing order requires Shah to obtain court approval before bringing new CIPA or related digital-privacy actions in the Central District. The order is significant, but it is narrow: it does not affect Shah's pending cases or prevent him from pursuing claims in state court, other federal districts, or arbitration. Still, the ruling gives businesses facing Shah's CIPA demands a significant new basis to challenge his credibility, motives, and litigation tactics in settlement discussions and contested proceedings.

In addition, the prospect of legislative reform has some momentum. California Senate Bill 690, which was originally introduced in 2025 but stalled in the Assembly, has been revived and substantially amended in July 2026. As currently drafted, the bill would eliminate the private right of action for alleged violations of CIPA's pen register and trap and trace provisions arising from conduct on websites and digital applications, leaving enforcement of those claims to the California Attorney General. The change would apply retroactively to certain pending actions filed within two years before the bill's operative date, potentially eliminating a substantial number of existing claims. The current bill is narrower than earlier versions, however, and would not affect claims under Section 631—the wiretapping provision underlying many CIPA website lawsuits and demand letters. SB 690 remains pending and may be further amended or fail to pass, so businesses facing current claims cannot yet rely on it for protection.

What To Do: Practical Guidance

A. If You Have Received a Demand Letter or Complaint

- **Do not ignore it—but also do not respond directly.** Many of these demands are structured to pressure the website operator into a quick settlement. They require a prompt, coordinated investigation of the claimant's allegations and the website's configuration

before deciding how or whether to engage.

- **Preserve evidence immediately.** Before modifying or removing any tracking tools, preserve screenshots, privacy disclosures, cookie banners, terms of use, consent records, tag-manager configurations, and available network-traffic or HAR files. Website configurations change frequently, and evidence of what information was transmitted, and when, may be critical to the defense.
- **Consider notifying relevant insurers.** Evaluate whether cyber, general liability, or other insurance coverage may apply to the claim and consider providing notice to any potentially responsive carriers.
- **Consult with counsel.** Reach out to counsel to evaluate the strength of the claim, the available legal and procedural defenses, and whether settlement, litigation, or arbitration is the most appropriate response.

B. Proactive Steps for Businesses That Have Not Yet Received a Demand

- **Audit your website's tracking technologies.** Identify all cookies, pixels, analytics tools, chat features, and session replay programs operating on the website. Determine what these tools collect, when they activate, where the information is sent, and what the recipient does with it.
- **Provide clear notice of the tracking technologies.** Disclosures, such as a cookie banner, should accurately identify the categories of information collected, the third parties receiving it, and the purposes for which it is used. Generic statements that a website uses cookies to "improve the user experience" may not adequately describe disclosures made for advertising, analytics, or other third-party purposes. If your website uses technologies such as Google Analytics that continue to collect anonymized utilization or user-behavior data even after a visitor selects "reject all," ensure that your cookie banner or consent management platform provides clear notice of the collection of analytics information.
- **Confirm that consent mechanisms work in practice.** A cookie banner is useful only if the website's technical behavior matches the choices presented to visitors. Test whether nonessential tracking tools activate before consent, whether rejecting cookies actually prevents transmission, and whether later changes to a visitor's preferences are honored.
- **Align disclosures with actual practices.** Ensure that privacy policies and cookie notices accurately describe the tools in use and periodically retest and document the website's configuration as technologies change.

If you have questions about CIPA compliance or have received a demand letter or complaint raising website privacy concerns, please contact the attorneys listed below or anyone on Tucker Ellis's Privacy & Data Security Team.

Additional Information

For more information, please contact:

- Alexander R. Safyan | 213.430.3031 | alexander.safyan@tuckerellis.com
- Roylance L. Bird | 213.430.3410 | lance.bird@tuckerellis.com