



CIPA Website Tracking Lawsuits: Where the Law Stands, Where It's Going, and What Your Business Should Do Now

If your website runs analytics, advertising pixels, chat widgets, session replay tools, or virtually any third-party tracking technology, you are operating inside one of the most aggressive privacy litigation environments in the world. California's Invasion of Privacy Act (CIPA), a 1967 statute originally enacted to address telephone wiretapping and other forms of eavesdropping on confidential communications, has become the vehicle for thousands of demand letters and class actions targeting websites.

But the legal ground is deeply uncertain. A federal judge approved a \$3.85 million class settlement against the *Los Angeles Times* on June 26, 2026. Just three weeks earlier, a California state court dismissed a near-identical claim with prejudice. Meanwhile, the Second and Sixth District's Courts of Appeal are preparing to issue the first appellate rulings on whether CIPA reaches website tracking technologies at all. Not to be outdone, the California legislature is currently considering a bill that could moot most CIPA claims.

This article explains where the law currently stands, why credible defendants choose to settle, why the legal foundation driving those settlements is starting to crack, and what your business should do today.

The Statute and the Theories

Two CIPA provisions do most of the work in current litigation.

- **Section 631(a) – the wiretap theory** prohibits a third party from reading or attempting to read the contents of a communication while it is in transit, without consent. Plaintiffs argue that information typed into a search bar or web form is protected “content,” and third-party trackers capturing it are illegally intercepting communications.
- **Section 638.51 – the pen register theory** prohibits the use of a pen register or trap-and-trace device without a court order or under limited statutory exceptions. Plaintiffs argue that tracking pixels and analytics tools collecting IP addresses, device identifiers, and routing information are the digital equivalent of a pen register – capturing the metadata of a visit rather than its content.

CIPA authorizes statutory damages of \$5,000 per violation or three times actual damages, whichever is greater. Plaintiffs commonly argue that each website visit – and in some cases each data interception – counts as a separate violation.

CIPA Reaches Beyond California

CIPA’s protection follows the California resident, not the business. When a California resident visits a website and tracking technology captures information from that visit, the statute attaches to the California-side communication – regardless of where the business is located, who it markets to, or how it sees its audience.

Any business operating a website should assume CIPA exposure. Disclaiming California intent in the privacy policy or terms of service is not a defense to a claim. The defenses that may work – consent obtained before any tracker fires, accurate privacy policies, or contestable jurisdictional facts – are heard in a motion to dismiss or on the merits. The geographic intent of the website owner is generally irrelevant.

Why Litigation Is Surging

Three structural features have produced the current wave of filings.

1. **The economics favor the plaintiffs.** Statutory damages give plaintiffs a credible damages model without proving individual harm. Indeed, actual damages would otherwise likely be difficult to prove. Understanding this dynamic, plaintiffs calibrate settlement demands to be below the cost of defending the case.

2. **The case law is unsettled.** California state courts increasingly find that web tracking technologies are not within CIPA's pen register controls. In contrast, federal courts in California have largely held that they are covered. Because no California appellate court has issued a decision on the issue, the federal courts do not consider themselves bound by the state-level trial courts. This split makes the outcomes hard to predict.
3. **Two parallel litigation streams are feeding the surge.** Plaintiffs' class action firms file substantial class actions seeking multimillion-dollar settlement funds. At the same time, pro se plaintiffs, most notably Vivek Shah, send waves of individual demand letters to businesses across the country, demanding settlements small enough to make litigation uneconomical.

Vivek Shah is the most common plaintiff and typically sends pre-litigation packets to companies across the country, each engineered to look like a ready-to-be-filed lawsuit. The packets typically include a cover letter requesting Informal Dispute Resolution, a draft complaint for Los Angeles Superior Court, which is nearly identical for all recipients, and Exhibit A screenshots showing tracking information being transmitted in real time to third-party tools like Google Analytics, Meta Pixel, and HubSpot.

The result is a litigation environment where a business may face a class action, an individual demand letter from a pro se plaintiff, or both, over essentially the same website configuration.

The Mirmalek Settlement: A Case Study

On June 26, 2026, the U.S. District Court for the Northern District of California granted final approval to a \$3.85 million class action settlement against the *Los Angeles Times* (*Mirmalek v. Los Angeles Times Communications LLC*¹).

The case targeted three specific trackers on the *LA Times* website and mobile apps: TripleLift, GumGum, and Audiencerate. The plaintiff alleged the trackers collected information without consent in violation of CIPA §638.51(a) – the pen register theory.

Three details are worth noting:

1. **The LA Times did not concede liability.** It settled to avoid the cost and uncertainty of continued litigation.
2. **The plaintiff acknowledged risk.** In response to an objection characterizing the CIPA claim as “well-worn,” the class representative argued the pen register theory was novel and risky, citing a pending California Courts of Appeal case and proposed legislation as the reasons.
3. **This was a strategic decision.** This was a calculated decision to resolve a novel-theory class action rather than continue to litigate amid genuine legal uncertainty.

What makes *Mirmalek* significant is precisely the gap between its outcome and the current state of CIPA litigation.

The Splits and the Dismissals

While *Mirmalek* was being settled, other California courts were dismissing similar claims.

*Rodriguez v. Ink America Int’l Group LLC*², a Los Angeles Superior Court judge dismissed §638.51 claims without leave to amend, holding the statute was designed for telephonic-style surveillance rather than commercial website operation. The court reasoned that upholding the plaintiff’s interpretation would criminalize conduct the CCPA expressly permits.

*Heiting v. Wildflower Brands*³ dismissed an entire CIPA complaint with prejudice on similar reasoning, noting that the internet was in widespread use when the relevant provisions were enacted in 2015, and the legislature said nothing about websites.

Balabbo v. Wildflower Brands, decided 10 days before *Heiting*, reached the same result on CIPA but allowed a common-law invasion of privacy claim to survive – a reminder that even when CIPA fails, sensitive data flows can keep a case alive on other theories.

*Blaker v. Netscout Systems*⁴, reinforced the trend, dismissing §638.51 claims against an SDK deployment with prejudice. The court emphasized §638.52’s court-order prerequisite, which makes sense in a telephone surveillance context but not in a

website context, as further evidence the statute was not intended for the conduct at issue.

Federal courts in California have been less consistent – *In re USA Today Co. Internet Tracking Litigation* dismissed a §638.51 claim, while other federal courts have let similar claims proceed at the pleading stage.

Despite allowing some cases to proceed, federal courts have constrained the most prolific pro se demand letter campaign. In *Shah v. Talentbridge, Inc.*⁵, Vivek Shah had alleged that a website's sharing of generic search terms that he typed violated his privacy rights. The Central District of California dismissed Shah's CIPA claim on two independent grounds: lack of Article III standing and failure to allege diversity jurisdiction. Most importantly for other potential defendants, the court held that typing generic search terms into a public website did not implicate a protectable privacy interest. The court denied Shah leave to amend as futile. For businesses receiving Shah-style demand letters, *Talentbridge* is meaningful – reflexive settlement may not be the best response when the underlying theory cannot survive a standing challenge.

The pattern is real but uneven. California state courts have been increasingly willing to hold that §638.51 simply does not reach website tracking. California federal courts have remained more willing to let these claims proceed at the pleading stage, though that consensus is also fraying.

The Pending Court of Appeal Case: Variety Media

Every dismissal discussed above is a trial court ruling. None creates binding California precedent. That could change soon.

*Variety Media, LLC v. Superior Court*⁶ is pending before the California Court of Appeal for the Second Appellate District. The case directly asks whether a website pixel qualifies as a pen register under CIPA §638.51. Major business groups, including the Association of Corporate Counsel, have filed amicus briefs arguing that applying CIPA to routine website operations would cause “operational paralysis.”

A second appellate case, *Reuters News & Media, Inc. v. Superior Court* in the Sixth Appellate District, will address essentially the same question.

Either appellate court could be the first California appellate authority to rule on whether CIPA §638.51 reaches website tracking technologies. A decision in either could take roughly a year from when briefing closed. Defendants currently facing pen-register-only claims therefore have a real strategic question to consider: settle now at uncertain pre-appellate prices or wait.

The Pending Legislation: California SB 690

The other risk the *Mirmalek* plaintiff identified is California Senate Bill 690, which would amend CIPA to add a broad “commercial business purpose” exemption that would effectively end most website tracking class actions. While SB 690 stalled in 2025, it is moving again. On July 1, 2026, the Assembly’s Privacy and Consumer Protection Committee heard testimony on amended language from the bill’s sponsor, Senator Anna Caballero, and the changes meaningfully improve its odds of passing.

The amended bill now applies only to Sections 638.50 and 638.51, the pen register and trap and trace provisions. Section 631 wiretap claims are untouched. The bill also eliminates the private right of action under those two sections, shifting enforcement to the California Attorney General.

Retroactivity is back, reaching two years. Senator Caballero defended this by noting that filings under Section 638.51 grew from roughly 600 to more than 4,000 since the bill was introduced, many from just four plaintiffs’ firms using repeat plaintiffs. She said the surge reflected an attempt to file before a deadline, and, in her view, retroactivity would prevent that behavior from being rewarded.

According to legislative estimates, pen register and trap and trace claims now make up roughly two thirds of active California privacy litigation. The amended bill received substantial support at the hearing, though several remaining sections leave Section 631 claims unaddressed. SB 690 still has procedural steps ahead, but its trajectory has changed significantly.

For businesses facing or considering settlement of a Section 638.51 claim, the loss of the private right of action and the two-year retroactivity window are variables worth tracking as the bill moves through the Assembly.

What Businesses Should Do Now

The unresolved legal questions do not change the immediate compliance posture. Whether or not the Court of Appeal narrows §638.51 or SB 690 passes, several actions remain prudent for any business operating a website.

- **Know what your website actually collects.** Many business owners do not – the technology was installed by a web designer, agency, or hosting platform without explanation. That does not change the exposure. Depending on the types of data you are collecting, you may choose to limit that data or ensure you have received consent before collecting it (see below).
- **Know where the data you collect goes.** Selling data is an important consideration for many privacy laws, but sharing data with third parties, even if not directly for money, can be an equally important consideration.
- **Get consent before any tracker starts.** The recurring pattern in adverse rulings is the same: trackers firing before any consent is obtained. A consent banner shown after tracking has begun functions as disclosure, not consent. Websites should therefore ensure that they use a consent banner and that their trackers do not start until after the user consents.
- **Confirm your privacy policy matches actual data flow and California exposure.** Generic policies that do not match what your site does provide no real defense. Keep in mind, CIPA follows the California visitor – disclaiming California intent is not necessarily a defense.
- **Do not assume reflexive settlement is the right answer.** Defendants facing pen-register-only claims with no §631 component may have meaningful reasons to test the law rather than pay. That decision requires real analysis of the specific complaint, the venue, and the underlying website configuration.

Where This Lands

The current state of CIPA website tracking litigation is unstable in both directions. Plaintiffs have extracted thousands of small, 5-figure settlements as well as high profile multimillion-dollar settlements from credible defendants using theories that

may not survive appellate review. At the same time, some defendants have won outright dismissals in cases that, under settled precedent six months ago, would have produced settlements.

What is not unstable is the obligation of any business operating a website to know what it collects, where the data goes, and what it has disclosed to the people being recorded. That obligation does not depend on how the Court of Appeal rules or whether SB 690 passes. It depends on the basic legal architecture that should have been in place before any tracker was installed.

The businesses best positioned, whether facing a Shah-style demand letter, a class action, or no claim at all, are the ones treating their website's data practices as a current legal compliance matter rather than a problem to address later.

The path through this environment is not luck. It is preparation.

If your business has received a CIPA demand letter or is concerned about its website tracking exposure, contact our firm for a confidential evaluation of your specific situation.

This blog was drafted by [Alexandra Samofalova](#), an attorney in the Spencer Fane Santa Monica, California office and a member of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.

1

No. 3:24-cv-01797-CRB

2

LASC 25STCV153 (Dec. 10, 2025)

3

April 2026

4

Case No. 25STCV31283 (May 27, 2026)

5

2026 WL 1507888 (C.D. Cal. May 28, 2026)

6

Case No. B350578

Click [here](#) to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.