Hashed & Salted | A Privacy and Data Security Update
May 2026

The Millisecond Problem: How Pre-Consent Tracking Is Driving CIPA Lawsuits in 2026

What began as a niche theory in California privacy litigation has, by early 2026, become a fast-moving plaintiff playbook. For in-house counsel at companies that collect consumer data through websites—retail, ad tech, hospitality, automotive and beyond—the risk is no longer theoretical. It is operational, technical and, increasingly, immediate.

At the center of this shift is the California Invasion of Privacy Act (CIPA), particularly Section 631 (wiretapping) and Section 638.51 (pen register). Plaintiffs are using these provisions to challenge routine web tracking practices—tracking pixels, website cookies, session replay, keystroke monitoring software—on the theory that they capture or transmit user communications without proper consent. The statutory damages of up to $5,000 per violation, potential of class action certification and inconsistent court rulings on how CIPA applies to online tracking make these cases appealing to the plaintiffs' bar and their clients.

CIPA claims typically begin with a demand letter containing these allegations and lead to settlement, a demand for arbitration or formal litigation.

While earlier cases debated whether pixels or cookies could ever constitute "interception," the 2026 cases assume those possibilities and instead focus on a narrower, more practical question: When, exactly, did tracking occur relative to user consent? A user lands on a webpage and before they interact with a banner or consent management platform (CMP), third-party tracking technologies—often Meta, TikTok or Google tags—fire and transmit data to third parties.

Plaintiffs argue that the sequence is dispositive: Consent must be obtained before any interception occurs. If tracking begins on page load, the unlawful interception occurred before the user had the opportunity to act.

The second theory being alleged is what courts have begun to describe as the "broken banner" scenario. Here, the user is presented with a cookie banner or CMP, actively declines or toggles off categories of cookies, and is told their preferences will be honored. Plaintiffs then allege their choices were not honored and that tracking continues.

A recent 2026 order in federal court describes precisely this situation: The website "set an expectation that user data would not be collected, but then collected it anyway." This framing is concerning for companies. It transforms what might otherwise be a technical compliance issue into something that sounds like an intentional mismatch or deception—opening the door not only to CIPA claims but also to unfair competition and misrepresentation theories.

Attorney Advertising

The third pattern alleges no meaningful consent mechanism at all. Plaintiffs allege that tracking technologies operate without any prior disclosure or authorization. These cases often emphasize Section 638.51, arguing that pixels and similar tools function as pen registers by capturing routing or addressing information such as IP addresses and identifiers. Courts remain divided on whether this analogy ultimately holds, but many are allowing these claims to proceed past the pleading stage.

These three theories are being tested in a growing number of 2026 filings, including recent actions in the Northern District of California. Across all three patterns, one development stands out: Plaintiffs are now routinely pleading wiretap and pen register claims together, often alongside federal Electronic Communications Privacy Act and common law privacy claims. This "stacked" approach increases leverage and complicates early dismissal strategies. At the same time, courts—particularly in federal districts—are showing a willingness to let these cases proceed into discovery, even where the legal theories remain unsettled. Yet the trend is not uniform. Most recently, the Central District of California dismissed a class action, *Travis Rounds v. Development Dimensions International*, that sought to extend CIPA liability to standard browser tracking, a ruling that may reflect an emerging willingness among some courts to examine more critically whether routine tracking technologies give rise to viable wiretap or pen register claims at the pleading stage.

None of this means that defendants lack viable arguments. Challenges to standing, the scope of "contents" under Section 631 and whether pixels qualify as pen registers remain active and, in some courts, successful. The "service provider" and "ordinary course of business" defenses also continue to play a role. But these arguments are increasingly being tested against a factual record that begins with how the website actually behaves at the moment of user interaction.

The trajectory is clear. Plaintiffs are moving toward claims that are easier to explain and harder to dismiss: The user said no and the website proceeded anyway; the user had not yet said anything and the website had already begun tracking. For companies operating consumer-facing websites, the risk is no longer confined to edge cases or unusual configurations. It sits in the ordinary functioning of digital marketing and analytics infrastructure.

For in-house counsel, the practical implication is that defensibility now turns less on legal positioning and more on technical reality. The critical questions are no longer abstract:

- Do any tags fire before consent is obtained?
- Are opt-out signals—whether via banner selection or Global Privacy Control—actually honored in real time?
- Does the behavior of third-party vendors align with the representations made in the privacy interface?

These are not questions that can be answered from policy documents alone. They require coordination with engineering, marketing and analytics teams, and often a granular understanding of tag management systems, firing sequences and vendor configurations. In litigation, plaintiffs are increasingly alleging—and seeking discovery into—precisely these details.

In our experience, companies can take action to increase their defensive posture by (1) maintaining a clear inventory of all tracking technologies on the site and understanding what runs, when it runs and what data is collected or shared; (2) reviewing and refining data minimization practices to avoid pen register claims; and (3) ensuring that their website's banner and CMP are regularly audited for proper functionality.

The quiet but important shift in 2026 is this: CIPA exposure is no longer primarily a question of whether you have a banner. It is whether your systems do exactly what that banner promises at the precise moment it matters.

Related Professional

Allison Cohen . . . . . ahcohen@loeb.com