

COURTS STILL DIVIDED ON WHETHER CALIFORNIA PRIVACY LAW APPLIES TO WEBSITE TRACKING: 4 RULINGS IN 10 DAYS HIGHLIGHT BUSINESS CONFUSION

Insights
Apr 21, 2026

Courts Still Divided on Whether California Privacy Law Applies to Website Tracking: 4 Rulings in 10 Days Highlight Business Confusion

If you were hoping the courts would offer clarity to the wave of California privacy litigation targeting website tracking technology, four decisions issued in just 10 days this April suggest you may be waiting a while. Four judges recently tackled nearly identical questions about whether the California Invasion of Privacy Act (CIPA) applies to the kind of third-party tracking tools that millions of websites use every day – and reached strikingly different conclusions. Here is what employers and businesses need to know about this eye-opening spate of rulings.

The Core Legal Question

At the heart of all four cases is the same statute: [CIPA's pen register and trap and trace provisions](#). Plaintiffs across the country have been filing suit arguing that common website tools like session replay software, third-party advertising trackers, and analytics platforms constitute illegal “pen registers” or “trap and trace devices” under CIPA because they capture information about website visitors without their consent.

The litigation wave has been enormous, and our [Digital Wiretapping Map](#) tracks just how broadly these suits have spread across industries and defendants. The four decisions

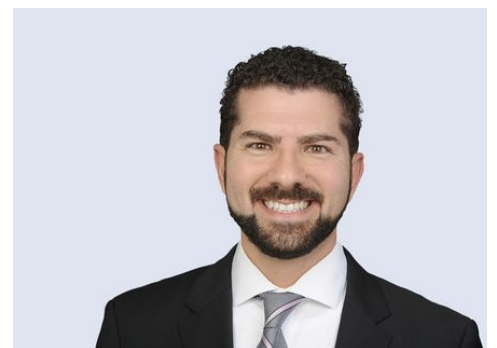
Related People



**Risa B. Boerner, CIPP/US,
CIPM**

Partner

610.230.2132



Usama Kahf, CIPP/US

Partner

below, all issued between April 6 and April 16, offer the most concentrated snapshot yet of where the law stands and how unsettled it remains.

Federal Court Keeps CIPA Claim Alive Against CNN

In *D'Antonio v. Cable News Network, Inc.*, a Southern District of New York federal judge denied CNN's motion to dismiss a CIPA class action arising from third-party trackers on CNN.com. The plaintiff alleged that CNN caused third-party trackers to be installed on visitors' browsers. Those trackers collected IP addresses, device metadata, and unique identifiers that were then matched against data broker profiles to de-anonymize users and sell targeted advertising, according to the suit.

The court found the plaintiff had adequately pleaded Article III standing, concluding that the **aggregation of tracking data into comprehensive, non-anonymous user profiles bears a close enough relationship to traditional privacy torts** (particularly intrusion upon seclusion) to survive dismissal. The court also rejected CNN's argument that the trackers collected communication "content" rather than the routing and addressing information covered by CIPA's pen register definition. Ultimately, the court declined to resolve that question at the pleading stage. The case now moves forward.

Federal Court Dismisses Nearly Identical Case Against USA Today

Just three days earlier, a Northern District of California judge reached the opposite conclusion in *In re USA Today Co. Internet Tracking Litigation*. The plaintiffs there alleged that USA Today embedded third-party trackers on its website that collected IP addresses, device type, browser type, and related metadata without consent, a fact pattern almost indistinguishable from the CNN case.

But this court dismissed the complaint for lack of Article III standing, finding that the specific data allegedly collected simply doesn't implicate a legally protected privacy interest under established 9th Circuit precedent. **IP addresses, device type, and browser type**, the court held, are not the kind of personal information where disclosure would be highly offensive to a reasonable person.

949.798.2118

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

SAME FACTS. OPPOSITE RESULTS.

Courts continue to split on whether CIPA applies to website tracking



CNN

CASE MOVES FORWARD

Court says data profiling could create real privacy harm



USA TODAY

CASE DISMISSED

Another court says same data not considered private enough



WILDFLOWER (BALABBO)
SPLIT DECISION

Court kicks CIPA claim out, but allows privacy claim to survive



WILDFLOWER (HEITING)
CASE DISMISSED (WITH PREJUDICE)

Court says CIPA not meant to govern website technology



California State Court Delivers a Split Decision Against Wildflower Brands

Back in state court, a Los Angeles Superior Court judge tackled CIPA claims against online retailer Wildflower Brands and delivered a mixed result. In *Balabbo v. Wildflower Brands*, the court sustained the defendant's challenge on the CIPA pen register and wiretapping claims. It found that CIPA's trap and trace provisions **don't apply to session replay technology** and that the CCPA and CPRA (California's comprehensive consumer privacy framework) govern website data collection. The legislature, the court reasoned, couldn't have intended to criminalize under CIPA the very data collection practices it carefully regulated and permitted under the CCPA.

But the plaintiff's common law invasion of privacy claim survived. The court found that allegations involving the capture and transmission of **credit card information and medical data** to third parties were sufficient to proceed to determine whether that conduct constitutes a highly offensive intrusion. Wildflower must answer that remaining claim.

A Second Judge Dismisses Identical Claims Against Same Defendant – Entirely

Just 10 days after the *Balabbo* ruling, a different Los Angeles Superior Court judge dismissed a **near-identical CIPA case** against Wildflower Brands entirely and with prejudice. In *Heiting v. Wildflower Brands*, the court concluded that CIPA's pen register and trap and trace provisions were

designed **exclusively for telephone surveillance, not commercial websites.**

The court pointed to the telephone-specific language in the portion of the statute that governs how law enforcement obtains authorization to use these devices as proof that the legislature never intended the statute to reach website analytics tools. The fact that the internet was already in widespread use when these provisions were enacted in 2015, and the legislature said nothing about websites, was telling. With no viable path to amendment identified, the court dismissed the complaint with prejudice.

What This Means for Your Business

The takeaway from these four decisions is not reassuring for businesses that were hoping the courts would converge on a clear answer. Whether a CIPA website tracking claim survives may depend heavily on which court is hearing it, which specific data was collected, how precisely the plaintiff pleads the injury, and whether the case lands in state or federal court. If you have a customer-facing website (particularly if it uses third-party analytics, advertising trackers, or session replay tools), you remain squarely in the crosshairs of this litigation.

Legislative reform may eventually bring more predictability. A coalition of businesses and trade groups has been pushing to clarify CIPA's scope and rein in the litigation surge — [and you can read more about those efforts and what they could mean for your business here.](#)

In the meantime, the best defense is a proactive one: audit your website's tracking tools, review your privacy disclosures, and make sure your consent mechanisms are up to date. [You can read our five-point list of suggestions here.](#)

Conclusion

To stay current on CIPA developments, legislative progress, and other California privacy litigation trends, subscribe to [Fisher Phillips' Insights](#). If you have any questions, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our [Digital Wiretapping Litigation Team](#).