

COURTS PUSHED BACK ON WEBSITE TRACKING LAWSUITS IN SEPTEMBER, BUT BROKEN COOKIE BANNERS ARE STILL A MAJOR RISK

Insights
Sep 30, 2026

Courts Pushed Back on Website Tracking Lawsuits in September, But Broken Cookie Banners Are Still a Major Risk

FP tracked six court rulings in September claiming that businesses illegally let third parties track visitors to their websites, with four favoring the companies being sued and two favoring plaintiffs. The cases were brought under California's wiretapping and "pen register" laws, along with similar federal and Pennsylvania statutes, and many of them turned on one question: did the site's cookie banner actually honor a visitor's choice to reject tracking? Two courts held that a broken opt-out button isn't enough on its own to keep these claims alive, and that plaintiffs still need to show that sensitive information was taken or that an actual communication was intercepted. But one decision went the other way on every issue – and a pending California appeal could decide whether the pen register law applies to websites at all. Here's what businesses need to know.

Quick Refresher: The Claims at Issue

- **CIPA Wiretapping (Penal Code Section 631):** Prohibits reading or learning the *contents* of a communication while it is in transit, and prohibits helping someone else do so. Plaintiffs usually argue that the website owner aided third-party tracking vendors.

Related People



Usama Kahf, CIPP/US
Partner

949.798.2118

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

- **CIPA Pen Register (Penal Code Section 638.51):** Prohibits installing a device or process that records “dialing, routing, addressing, or signaling information” without a court order. It expressly excludes the contents of a communication. Plaintiffs argue that tracking cookies and pixels qualify.
- **Federal Wiretap Act:** A one-party consent law. Because the website is a party to the communication, a claim against the site owner only works if the interception was done to commit a separate crime or tort.
- **Standing:** To stay in federal court, plaintiffs must show a concrete injury. Courts measure privacy injuries against traditional claims like intrusion upon seclusion, which requires an intrusion that is “highly offensive” to a reasonable person.

California’s CIPA allows statutory damages of \$5,000 per violation without proof of actual harm, which is why these suits keep coming. You can track the spread of this litigation on [FP’s Digital Wiretapping Litigation Map](#).

The “Broken Cookie Banner” Theory

Many recent suits share a fact pattern. A website offers a “Reject All” or “Do Not Sell My Personal Information” button, a visitor clicks it, but third-party tracking keeps running anyway. Plaintiffs argue that the banner created an expectation of privacy, and that ignoring the visitor’s choice turns ordinary tracking into deceptive, “highly offensive” conduct. Five of the six decisions below involved some version of this allegation. Courts disagreed about how much that matters.

✓ Wins For Businesses

September saw four very good decisions for businesses that you should follow.

***Lutge v. Timex* (N.D. Cal., Sept. 14): A broken banner doesn’t make ordinary data sensitive**

Judge Edward Chen dismissed a CIPA and federal wiretap suit against Timex on standing grounds, even though Timex never raised standing in its motion. The court took up the

issue on its own because federal courts have an independent duty to confirm they have jurisdiction.

The plaintiff said he rejected cookies, bought a watch, and that Timex still passed his purchase details and email address to a third party that allegedly used “identity resolution” to link anonymous visitors to profiles built from data collected across many other websites and devices.

While Judge Chen agreed that deceit can be a “plus factor” that elevates borderline conduct, he held that it doesn’t turn routine data collection into a highly offensive intrusion. “The key is the sensitivity of the information collected,” the court said, and a shopper’s name, email address, and watch-browsing and purchase activity did not qualify.

The court distinguished cases involving health and fertility data, and noted that the plaintiff hadn’t alleged the third-party data collector actually built anything resembling a comprehensive “cradle-to-grave” profile. The dismissal was without prejudice, so the plaintiff can try again. But the ruling directly undercuts the argument that a faulty cookie banner creates standing by itself.

***Wiley v. Universal Music* (N.D. Cal., Sept. 14): Clicking around a website isn’t a “communication”**

On the same day in the same jurisdiction, Judge P. Casey Pitts dismissed the plaintiffs’ CIPA wiretap and pen register claims with prejudice in another case after they failed to fix the problems he identified in their first complaint.

On the wiretap claim, the plaintiffs alleged that third parties received full-string URLs showing that they had viewed Post Malone tour dates and merchandise pages, along with session data, device information, and button clicks. The court held that this is browsing information, not the “contents” of any communication. The plaintiffs had even excluded search queries from their allegations. In the court’s words, they alleged only that they visited particular pages, “not that they communicated anything in particular to those websites.”

The pen register claim failed for a related reason. A pen register captures routing and addressing information tied to a communication, so the plaintiffs argued their communications were captured when they were visiting the websites. But as the court put it, “mere browsing activity is

not analogous to a phone call," because calls are communicative and browsing generally is not.

***Negrete v. ScentAir Technologies* (L.A. Superior Court, Sept. 16): Collecting an IP address isn't a crime**

A few days later, a Los Angeles trial court rejected a pen register claim brought by a self-described privacy "tester" represented by Pacific Trial Attorneys, a firm that has filed many of these suits. The plaintiff alleged that tracking tools fired on ScentAir's site even after he rejected all third-party cookies.

The court found that the only specific conduct alleged was the collection and transmission of the plaintiff's IP address. Because that happens every time anyone visits any website, the court said it "would be absurd to interpret the pertinent CIPA provisions to criminalize the process by which all websites communicate with all users who voluntarily elect to access them." The court also noted that the pen register law was written to govern law enforcement telephone surveillance, pointed to the statute's exception for service providers operating in the ordinary course of business, and held that users have no reasonable expectation of privacy in their IP addresses.

The plaintiff has 30 days to amend, and trial court rulings don't bind other courts. Still, the reasoning gives defendants a useful template for IP-address-only pen register claims.

***Felsen v. Vanguard* (E.D. Pa., Sept. 15): No federal wiretap claim without a separate wrong**

A Pennsylvania federal court dismissed the plaintiffs' federal Wiretap Act claim against Vanguard, which allegedly allowed third parties to capture users' stock searches and trades. Because Vanguard was a party to the communications, the plaintiffs needed to show the interception was for the purpose of committing a separate crime or tort. They argued that the data was later assembled into advertising profiles. The court held that they never explained how that amounted to an independent wrong, and that binding 3rd Circuit precedent bars relying on the interception itself. The dismissal was without prejudice.

Where Plaintiffs Gained Ground

But it wasn't all good news. There were a few negative rulings to track as well.

***Spears v. The Campbell's Company* (N.D. Cal., Sept. 8):
The broken banner carries the day**

Magistrate Judge Thomas Hixson denied the defendants' motion to dismiss in full, with the faulty cookie banner theory discussed above playing a major role. The plaintiffs alleged that Campbell's website let third parties keep tracking visitors after they rejected cookies.

On standing, the court held that letting third parties collect users' data after telling them they could opt out supports a concrete and potentially highly offensive injury. The court also reworked the 9th Circuit's familiar comparison of website tracking to a store clerk watching shoppers. Here, it said, it would be as if the clerk promised shoppers they wouldn't be tracked, then secretly attached devices so third parties could follow them outside the store for a year or more.

On the CIPA claims, the court held that the plaintiffs plausibly alleged real-time interception while communications were in transit, and declined to dig into whether data was technically in "storage" first. It read the pen register statute's plain language to cover electronic communications generally, not just telephones. It also rejected the argument that a tool collecting contents can't also be a pen register.

Finally, the court refused to pause the case while the California Court of Appeal decides *Variety Media v. Superior Court*, which will address whether the pen register law reaches website software. [You can read all about that pending decision here.](#)

***D'Antonio v. Smith & Wesson* (N.D. Cal., Sept. 8): Search queries revive dismissed claims**

Six days before his *Universal Music* ruling, Judge Pitts revived CIPA wiretap and pen register claims he had previously dismissed against Smith & Wesson. This time, the amended complaint alleged that the plaintiffs typed searches into the site's search bar for t-shirts, a specific handgun model, holsters, and other accessories. Those queries were things the plaintiffs communicated to the website, so they counted as contents.

The court also rejected the argument that plaintiffs must identify the specific cookie, transmission, or third party involved, reasoning that those details are in the defendant's hands before discovery. And it allowed the pen register claim to proceed based on general allegations that cookies captured port numbers, protocol metadata, and HTTP header data.

What Should Businesses Do Now?

- **Test your cookie banner.** Confirm that "Reject All" and similar options actually stop third-party tags from firing, including on first page load. A broken opt-out was the deciding fact in *Campbell's*.
- **Map what leaves your search bars and form fields.** Courts are most willing to find "contents" in typed queries, so know which vendors receive that data.
- **Look harder at sensitive pages.** Financial, health, and similar information makes standing much easier to establish.
- **Review your data broker and identity resolution tools.** *Timex* survived these allegations, but only because the underlying data wasn't sensitive.
- **Don't rely on a choice-of-law clause.** *Vanguard* shows courts may apply CIPA to California users regardless.
- **Raise defenses early.** Standing and "contents" arguments are winning in some courts, and it's worth pressing both at the pleading stage with counsel.

Conclusion

We will continue to monitor developments in website tracking litigation, including the *Variety Media* appeal, and provide updates as warranted. Make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any member of our [Privacy and Cyber](#), [Digital Wiretapping Litigation](#), or [Consumer Privacy](#) teams.