Fisher Phillips

Insights, News & Events

5 RECENT COURT RULINGS SHOW BUSINESSES HOW TO DEFEND WEBSITE TRACKING LAWSUITS: PRACTICAL LESSONS TO APPLY TODAY

Insights
Jul 15, 2026

5 Recent Court Rulings Show Businesses How to Defend Website Tracking Lawsuits: Practical Lessons to Apply Today

Four courts issued five rulings in three weeks this June on website tracking lawsuits, offering a playbook you can use to minimize your chances of getting sued and defending yourself when you do. The rulings addressed the same underlying question: How much detail does a plaintiff need to survive a motion to dismiss or a demurrer over website tracking pixels, cookies, and third-party ad tech? Here's what happened, and more importantly, what businesses should do about it both before they're sued and after.

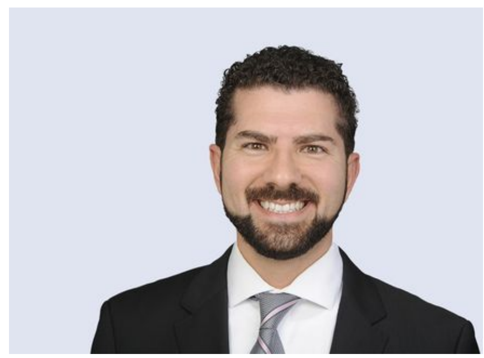
Why Some Claims Survived and Others Didn't

Between June 11 and June 30, the Northern District of Illinois, the Central District of California (twice, in two unrelated cases), the District of Massachusetts, and a California Superior Court all issued rulings in five cases that addressed one of the thorniest issues facing business today: the extent to which digital wiretapping claims can be brought against businesses for commonplace tracking activity. You can track the explosion of these lawsuits on FP's Digital Wiretapping Litigation Map.

Here's a recap of each case and why some survived and some didn't.

Vagueness Killed 2 Claims

Related People



Usama Kahf, CIPP/US

Partner

949.798.2118

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

In *Watson v. Franciscan Alliance* (N.D. Ill., June 11), a hospital system patient alleged that a third-party ad platform intercepted her communications with the hospital's website. Her general allegations about the tracking technology were detailed. But the details about herself were not.

- She didn't allege specific diagnoses, specific treatments, or that she'd scheduled any appointment through the site.
- She also never alleged she'd received targeted advertising afterward, the kind of circumstantial factual allegation courts have accepted elsewhere as sufficient at the pleading stage to show that personal data was actually disclosed.

The court dismissed for lack of standing, emphasizing that a named plaintiff in a class action must show she personally was injured, not that unnamed class members were.

The same defect sank half of *Cheung v. Slickdeals* (C.D. Cal., June 29). Plaintiff Nina Harris alleged that Slickdeals' tracking tools captured her "browsing activity" and "page interactions" and shared them with ad tech platforms. The court found this insufficient. Without specifics about what personal information was actually collected, the court could not find a harm resembling the common law tort of intrusion upon seclusion. Her California Invasion of Privacy Act (CIPA) and unfair competition claims were dismissed, with leave to amend.

Specificity Saved 3 Claims

The other plaintiff in the same *Slickdeals* case fared very differently. Andrew Cheung alleged he'd purchased four named video games through the site, that his purchase activity and Facebook ID were transmitted to an ad tech website, and that he began receiving targeted ads for the same content afterward. That was enough. The court found he'd adequately alleged an injury analogous to intrusion upon seclusion, specifically a violation of his reasonable expectation of privacy in his video-viewing history, and let his Video Privacy Protection Act (VPPA) and Wiretap Act claims proceed.

Firlej v. Petrosian Esthetic Enterprises (C.D. Cal., June 18) followed the same logic in a medical context. The plaintiff didn't just allege generic browsing data was captured, but instead alleged the tracking pixel transmitted information that she'd scheduled a specific type of appointment and the reason for it. That specificity carried her invasion of privacy, negligence, Electronic Communications Privacy Act, and CIPA claims past the motion to dismiss stage, even though her breach of implied contract claim was dismissed for lack of consideration.

Saul v. Valnet (D. Mass., June 30) reinforced the point outside California entirely. The plaintiff identified the exact video titles he'd viewed on a gaming website and alleged his account ID was linked to that activity and disclosed to an ad tech website. That level of detail was enough not just to state a VPPA claim, but to help establish personal jurisdiction over a Canadian corporate defendant under the Fifth Amendment's more flexible due process standard.

Consent Defenses Are Struggling at the Pleading Stage

Three of the five rulings rejected consent-based defenses outright, and for a common reason: the businesses hadn't put the actual consent documentation properly in front of the court.

- In a June 16 California Superior Court ruling, the court overruled a demurrer premised in part on a consent defense, holding that consent is an affirmative defense that can only defeat a claim at the pleading stage if it's conclusively established by the face of the complaint. It wasn't here.
- In *Firlej*, the defendants never formally requested judicial notice of the ad tech company's privacy policy, raising it only in a reply brief footnote, which the court called improper. Even considering the cited language, the court found it too vague to establish that the plaintiff had consented to the specific data-sharing at issue.
- In *Saul*, the same problem surfaced again. The complaint didn't reference Valnet's privacy policy at all, and the court declined to consider a document outside the pleadings at the motion to dismiss stage. The court also noted that even if it had considered the policy, nothing in it established that the statutory requirements for VPPA consent, including specific timing and form requirements, had actually been met.

VPPA Is Stretching Further Than Expected

The *Slickdeals* ruling contained a holding that deserves attention well beyond media and streaming companies. Slickdeals argued it wasn't a "video tape service provider" under the VPPA because it never hosts or sells video content directly. It merely lists deals and directs users to external retailers to complete their purchases.

The court rejected that argument, holding that **earning a commission on sales**, including sales of video games and other audiovisual content, **is enough to be "engaged in the business"** of selling that content under the statute. Multiple parties can be engaged in the business of selling the same content, the court reasoned, and an affiliate or referral relationship doesn't insulate a business from VPPA exposure.

What Businesses Should Do Before Litigation

- **Audit what your trackers actually transmit, not just whether you have them.** Knowing you run an analytics program through a third-party website isn't enough. Know whether those tools are capturing identity-linkable specifics: account IDs tied to purchases, appointment types, exact URLs that reveal health information or other sensitive detail. Those are the exact data point courts are now using to separate viable claims from dismissible ones, and it applies just as much to your own risk exposure as to a plaintiff's.

- **Tighten your privacy policy's specificity.** Courts in three of these five rulings explicitly rejected generic "we may share data with partners" language as insufficient to establish consent. Vague disclosure that once felt like reasonable coverage is now being construed against the business that wrote it. Say plainly what's collected, what's shared, and with whom.

- **Reconsider affiliate and commission-based content links.** If your site earns revenue by directing users to purchase video content or other media elsewhere, evaluate your VPPA exposure now. The *Slickdeals* ruling suggests hosting the content isn't required for exposure to attach.

- **Get consent capture into proper form.** If consent is going to be part of your defense, make sure it's actual, specific, and documented, not a passive Terms of Service link a user never had to click through. Several of these rulings turned on the absence of any distinct, written, affirmative consent mechanism.

What Businesses Should Do During Litigation

- **Push hard on standing and specificity at the pleading stage.** If a complaint relies on generic language like "browsing activity" or "page interactions" without tying it to what the plaintiff personally searched, viewed, or received in return, that is currently a live and successful dismissal argument in multiple jurisdictions. Don't over-settle out of pattern-matching to unrelated, larger verdicts.

- **Get your privacy policy properly before the court, and do it early.** Multiple defendants in these rulings lost consent arguments not on the merits, but on process: failing to request judicial notice, or raising the policy for the first time in a reply brief. Consent defenses need to be teed up correctly from the opening motion.

- **Don't assume a profit motive defeats a crime-tort exception.** Courts are increasingly finding that a defendant's argument of "we were only trying to make money" doesn't automatically defeat the tortious-purpose exception to one-party consent under wiretap statutes. Build your defense strategy assuming that argument alone won't carry the day.

- **Expect the next wave of complaints to be more detailed.** Plaintiffs' counsel are visibly adapting in real time to exactly these rulings. Build motion-to-dismiss strategy assuming the next complaint you face will have already patched the specificity gaps that sank the weaker claims this time around.

Conclusion

Fisher Phillips will continue to track digital wiretapping litigation across the country. To stay current on CIPA developments and other privacy litigation trends, subscribe to Fisher Phillips' Insights. If you have questions about CIPA compliance or exposure, reach out to your Fisher Phillips attorney, the author of this Insight, or any member of the firm's Consumer Privacy Team or our Digital Wiretapping Litigation Team.