The Computer & Internet Lawyer

Volume 43 ▲ Number 6 ▲ June 2026

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Online Tracking Litigation: The Risks Keep Evolving

By Tyler G.D. Anders and Xeris E. Gregory

There are numerous names — like pixels, beacons and tags — and functionalities for online tracking technologies. However, there are three broad classes of third-party tracking technologies that primarily feature in lawsuits: analytics (including cross-channel and data enrichment technologies), chatbots and retargeting technologies. While all three types create legal risk, analytics and retargeting technologies are seen most frequently on websites and therefore in web-tracking litigation. Businesses leveraging these tools often use them to track user engagement and to re-engage prior website visitors.

SPECIAL ISSUES IN ONLINE TRACKING LITIGATION

The unifying theory in alleging that web technologies violate state or federal statutes is that tracking technologies allegedly disclose private information to third parties without consent. Despite this relatively straightforward premise, the legal landscape is still turbulent in how web-tracking lawsuits are handled.

The authors, attorneys with Polsinelli, may be contacted at tanders@polsinelli.com and xgregory@polsinelli.com, respectively.

Plaintiffs' firms have found repeated success in litigating web-tracking claims, causing disruption for businesses of all sizes and in every sector. This is based, in part, on the ease of access to the information needed to bring a claim and the strict liability penalties that accompany statutory violations.

In the past year, special issues have come to the forefront in these cases.

Standing

In web-tracking lawsuits, courts are increasingly requiring plaintiffs to show individualized harm to establish Article III standing. In other words, some federal courts are tightening the screws on "no-injury" cases.

First, courts are increasingly unwilling to find Article III standing where a plaintiff's only injury is an alleged statutory violation. Both the Third Circuit and the Ninth Circuit reiterated this principle in two separate web-tracking cases in August. The Third and Ninth Circuits affirmed dismissal in both cases, reiterating that "Article III standing requires a concrete injury even in the context of a statutory violation." In other words, merely alleging that a defendant's website violated a statute does not automatically mean a plaintiff has standing to sue. There must still be some real-world harm to the plaintiff.

Second, courts are also increasingly unwilling to find standing where the information allegedly transmitted by web-tracking technologies is not inherently private or sensitive. In both cases before the Third and Ninth Circuits, the plaintiffs alleged injury based on loss of privacy. However, the Ninth Circuit likened the defendant's monitoring of user interactions on its website to "a store clerk's observing shoppers in order to identify aisles that are particularly popular or to spot problems that disrupt potential sales." And the Third Circuit noted that "none of the information entered on the defendant's website was personal or sensitive." Thus, neither plaintiff had adequately alleged there was an invasion of privacy.

The takeaway from these recent decisions is that courts can be skeptical about plaintiffs in web-tracking lawsuits. It is not enough to simply allege that a website transmits information to a third party. Plaintiffs must also have suffered some real-world harm as a result. While these decisions offer hope on the horizon for businesses confronted with web-tracking demand letters or lawsuits, businesses should still be wary. The inquiry is still fact-specific, and the categories and type of information transmitted to third parties are crucial for determining whether a lawsuit can proceed past the motion-to-dismiss stage.

The Untenable State of the California Invasion of Privacy Act (CIPA)

Frustrations with the current application of CIPA — California's wiretapping statute first enacted in 1967 — in online tracking litigation came to a head last year for at least one federal district court judge. In *Doe v. Eating Recovery Center LLC*,[1] Judge Chhabria of the U.S. District Court for the Northern District of California called the "language of CIPA" a "total mess." Judge Chhabria noted that "it's often borderline impossible to determine whether a defendant's online conduct fits within the language of the statute." The problem, according to Judge Chhabria, is that "the statutory language was drafted with very different technology in mind, and it does not map properly onto the internet."

Two other decisions in the U.S. District Court for the Northern District of California echoed Judge Chhabria's frustrations, succinctly identifying the inherent contradiction at the heart of CIPA "trap-and-trace" lawsuits filed in California in recent years.

Judge Noël Wise addressed two trap-and-trace class actions involving allegations of CIPA violations through the defendants' websites' use of a TikTok tracking tool. Although the Court found that plaintiffs lacked Article III standing in both cases, its findings did not stop there. Judge Wise went on to find that the defendants' website and the related software did not constitute a "trap-and-trace device" as defined by Cal. Penal Code § 638.50(c).

Judge Wise summarized her reasoning as follows:

> If Defendant only collects information regarding the "metadata" of the communication, Plaintiff's right to privacy is not invaded because he has no expectation of privacy as to that type of data (e.g., his IP address or general geographic location). If Defendant instead collects content information from communication between the parties (e.g., information provided from Plaintiff to Defendant directly), then the TikTok software is not a trap and trace device and § 638.50 does not apply.

CIPA defines a "trap-and-trace device"[2] as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of the communication." By definition, a "trap-and-trace device" captures identifying information "about" a communication (i.e., the metadata) but not the "contents" of the communication. This distinction "crystalizes the futility of plaintiff's suit (and the myriad identical cases plaintiff's counsel has filed in both federal and state courts)" as it forces plaintiffs into a Catch-22. To sufficiently allege standing, a plaintiff must allege the at-issue device captured the contents of their communication. But, by doing so, § 638.50 would no longer apply because § 638.50 only applies when information "about" a communication is captured.

It remains to be seen whether the California legislature will ultimately take action to update the outdated language of CIPA. In the meantime, these recent cases should hopefully give companies another tool to use should they find themselves facing actions involving allegations of CIPA violations.

Expanding Scope of ECPA Claims

Plaintiffs have brought numerous class action lawsuits against health care entities alleging theories under the Electronic Communications Privacy Act (ECPA) where an alleged transfer of protected health information (PHI) to third parties through website trackers allegedly violated the Health Insurance Portability and Accountability Act, other similar state statutes and various common law torts.

Recently, plaintiffs have increased efforts to expand ECPA claims into new contexts, and some courts appear to be receptive to allowing these claims to proceed in these new contexts. For example, a judge in the

Northern District of California allowed a putative class action against a shoe retailer to proceed on claims under the federal Wiretap Act.

In denying defendants' motion to dismiss, the court found that plaintiffs plausibly alleged that the defendant "intentionally used" "intercepted" communications in violation of 18 U.S.C. § 2511(1) of the federal Wiretap Act and used those communications to support its targeted advertisement strategy, and that the "alleged disclosure and use of Plaintiffs' personally identifiable information for advertising, in contradiction to the commitments it made in its privacy policy," was "tortious."

Growing Circuit Split on the Meaning of a "Consumer" Under the Video Privacy Protection Act (VPPA)

The VPPA creates civil liability for any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider."[3] The VPPA defines a "consumer" as "any renter, purchaser or subscriber of goods or services from a video tape service provider."[4] In 2024, the Second Circuit in *Salazar v. NBA*,[5] construed the definition of "consumer" broadly, holding that a broad scope of individuals who may not have purchased video services could still be considered "consumers" under the VPPA. In 2025, courts continued to grapple with the meaning of "consumer," reaching different conclusions and leading to a growing circuit split on this issue.

On the one hand, the Seventh Circuit followed the Second Circuit's approach. The defendant operated a website where people can watch classic video programming. Plaintiffs alleged they "signed up" with the defendant and provided the defendant with their email addresses and zip codes. The court concluded that "when a person does furnish valuable data in exchange for benefits, that person becomes a 'consumer' as long as the entity on the other side of the transaction is a 'video tape service provider.'" Under the court's expansive reading, a "consumer" includes subscribers to any goods or services from a video-tape service provider.

On the other hand, the Sixth Circuit in *Salazar v. Paramount Global* reached the opposite conclusion. Looking at a "virtually indistinguishable complaint filed by the same plaintiff" in the Second Circuit's *Salazar v. NBA* decision, the court held that an individual is a "consumer" under the VPPA "only when he subscribes to 'goods or services' in the nature of 'video cassette tapes or similar audio visual materials.'" In other words, the court tethered the phrase "goods and services" to "audiovisual," rejecting the expansive reading applied by the Second and Seventh Circuits. VPPA litigation looks to remain unpredictable, as there is no indication this growing split will be resolved soon. Companies who operate websites that stream video should continue to look for ways to limit their liability, including obtaining consent from their users sufficient to satisfy the VPPA, assessing pixel usage and evaluating what information is collected from website users.

IN SUMMARY

Online tracking litigation remains active — but unsettled. Courts are tightening standing requirements, questioning how old statutes apply to new tech, and reaching different conclusions on key issues like VPPA scope, making this an area to watch.

Litigation involving online tracking is here to stay. But the persistence of online-tracking lawsuits does not necessarily reflect more stability in the evolving legal landscape. The number of plaintiffs' firms pursuing web-tracking suits grew during the past year, and web-tracking litigation continues to challenge businesses across industries.

Notes

1. Doe v. Eating Recovery Center LLC, Case No. 23-cv-05561-VC (N.D. Cal. Oct. 17, 2025).
2. https://www.leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=638.50.
3. 18 U.S.C. § 2710(b)(1).
4. See 18 U.S.C. § 2710(a)(1).
5. Salazar v. NBA, 118 F.4th 533 (2d Cir. 2024).