Legal Backgrounder

WASHINGTON LEGAL FOUNDATION
Keeping Free Enterprise Free

Vol. 41 No. 10 July 28, 2026

Post–*Popa v. Microsoft*, Courts in California Keep the Standing Bar High for Web-Tracking Claims

by Lawrence ("LB") Burns

Nine months ago, in *Popa v. Microsoft Corp.*, the U.S. Court of Appeals for the Ninth Circuit held that Article III standing requires more than a bare statutory violation when a plaintiff alleges only routine, non-sensitive web tracking.[1] That decision gave website operators something they desperately needed: a principled, workable standard for knocking out pixel-tracking suits before they balloon into expensive class action discovery. California federal courts are applying *Popa* seriously, and the recent decision in *Torres v. SeatGeek, Inc.* is the latest proof.[2]

Case Overview

Jose Torres filed a proposed class action in the Northern District of California alleging that SeatGeek used third-party tracking pixels to collect and share his personal information without consent. The complaint alleged that the trackers captured his IP address, approximate location, browser activity, and device metadata (Digital Data), then transmitted that data to the third parties, which matched it against pre-existing user profiles through fingerprinting and cookie synchronization. Torres allegedly received targeted ads on his social media after visiting the SeatGeek site. Torres did not create an account, complete a purchase, submit a form, or type a search query. Rather, his lawsuit rested entirely on the Digital Data collected during the visit. He asserted four claims: violation of the California Computer Data Access and Fraud Act (CDAFA), violation of the California Invasion of Privacy Act (CIPA) Section 638.51(a), invasion of privacy under the California Constitution, and common law invasion of privacy. In response, SeatGeek moved to dismiss on standing grounds. On May 22, 2026, U.S. Magistrate Judge Laurel Beeler of the Northern District of California granted the motion.[3]

Standing, Still the Gatekeeper

The court's analysis focused on Article III standing. Citing *Popa*, Judge Beeler applied the now-familiar framework: to establish a concrete injury in a privacy case involving intangible harm, a plaintiff must allege harm that bears a close relationship to harms traditionally recognized as actionable at common law, something akin to intrusion upon seclusion or public disclosure of

---

[1] *Popa v. Microsoft: Pivotal Ninth Circuit Ruling Narrows Wiretap Suits over Web Analytics*, WLF Legal Opinion Letter, Vol. 34 No. 15 (Oct. 6, 2025) (Stegmaier & Burns).

[2] *Torres v. SeatGeek, Inc.*, No. 25-cv-07118-LB (N.D. Cal. May 2026).

[3] *Id.*

Lawrence ("LB") Burns is a senior associate in the Emerging Technologies Group at Reed Smith, practicing in the firm's Century City, CA office.

private facts, not a mere statutory violation.[4]

The court acknowledged that Torres's allegations were "more robust than those in *Popa*," which involved a single pet supply website. Here, SeatGeek's trackers fed data to three separate third parties, each of which already held a profile on Torres and used the new data to further identify him. But the court held the line:

> The information that was collected — IP addresses, device make/model/OS, browser type, and cookie identifiers — is record information where there is no reasonable expectation of privacy.

As the court put it, "what remains is the tracking of metadata generated by a visit to a public ticket-resale site. Under *Popa*, this does not resemble any traditional common-law privacy tort."

Three Arguments, Three Losses

Torres advanced three alternative grounds for standing—the court rejected each. First, he argued that CIPA's private right of action itself supplies Article III standing, pointing to cases holding that IP address collection for targeted advertising constitutes a concrete injury under the statute. The court disagreed, reasoning that receiving a targeted ad, without more, is not a concrete injury based on the transmission of non-confidential information.

Second, Torres contended that even if each data point was innocuous, aggregating them across three major platforms, each with existing profiles, was qualitatively different from what happened in *Popa*. The court found the argument unpersuasive. *Popa* involved a single website; *SeatGeek* involved three platforms, which made the *SeatGeek* claim factually richer, but the data itself was the same category of non-sensitive browsing metadata. The court distinguished the cases where aggregation arguments have succeeded: those involved defendants compiling detailed profiles reflecting users' interests, habits, locations, and behaviors across vast networks of sites over extended periods. SeatGeek's trackers captured only the basic technical record of a single visit to a ticket website. That gap could not be bridged simply by pointing to the number of alleged recipients.

Torres's third argument was that SeatGeek unjustly enriched itself by monetizing his data, which he offered as a standalone basis for standing. The court was not persuaded. Without a plausible privacy interest in the underlying information, there is nothing unjust about what SeatGeek allegedly gained, and bare assertions that a company "unjustly enriched" itself are exactly the kind of conclusory pleading that does not survive a motion to dismiss.

A Note on CIPA's Scope

A noteworthy aspect of the ruling is what the court did *not* do. Judge Beeler firmly rejected SeatGeek's argument that CIPA's trap-and-trace provision applies only to telephone technology, not internet-based tracking pixels:

> Many defendants have taken SeatGeek's position that [CIPA] applies only to tracking technology for phones and not the internet. None have succeeded in this district. SeatGeek cites no controlling case stating otherwise. The court does not depart from these decisions.

The statutory scope question received additional clarity just days later, and again in defendants' favor. On May 27, 2026, Judge Gary Roberts of the Los Angeles County Superior Court

[4] *Popa v. Microsoft Corp.*, 153 F.4th 784, 789 (9th Cir. 2025).

sustained a demurrer and dismissed, with prejudice, a CIPA trap-and-trace claim premised on a website software development kit, holding that CIPA's pen register and trap-and-trace provisions apply "to telephonic communications and not to software on a commercial website." *Blaker v. NetScout Systems, Inc.*, No. 25STCV31283 (L.A. Super. Ct. May 27, 2026).[5] The court's analysis turned on two points: (1) the text of Penal Code section 638.52, which conditions pen register authorization on identifying a specific "telephone line," and (2) the Legislature's decision to enact section 638.51 in 2015 *without any reference to internet technologies* at a time when web tracking was already widespread. If lawmakers had intended the statute to reach commercial websites, the court reasoned, they would have said so. The demurrer was sustained without leave to amend, the court having concluded that the defect was one of statutory scope rather than deficient pleading.

Broader Implications

SeatGeek and *NetScout* together reinforce *Popa*'s framework and give website owners a cleaner picture of where the defense lines sit across both federal and state court. In federal court, non-sensitive Digital Data, including IP addresses, browser identifiers, device metadata, and cookie IDs, does not establish Article III injury. In state court, where Article III standing is not a threshold requirement, the statutory scope argument now has real traction: *NetScout* establishes that CIPA was not written to reach commercial website technologies. Taken together, the two decisions offer a two-track defense; in federal court, the standing bar; in state court, the statutory scope argument. Neither ruling is a complete answer on its own, but read together they signal that courts at both the federal and state level are applying these statutes as written rather than stretching them to fit the creative litigation theories plaintiffs' counsel have been advancing for years. So long as CIPA's private right of action remains intact, however, plaintiffs' counsel will keep filing, keep refining their complaints, and keep looking for the fact pattern that gets them past dismissal. Legislative reform remains the more durable answer.

What Comes Next

Torres v. SeatGeek is the most significant application of the *Popa* concrete-injury standard to date. It sends a clear message: even a factually layered tracking claim, one involving multiple platforms, cross-site deanonymization, and alleged targeted advertising, cannot clear the standing bar without sensitive data or deceptive conduct involved. For website owners defending this litigation, that is a meaningful and hard-won data point. The litigation environment is also shifting on other fronts. The Ninth Circuit has accepted an interlocutory appeal in *Drummer v. CoStar Group, Inc.*, specifically to address whether the routine transmission of IP addresses establishes Article III injury under CIPA, the same question that controlled *SeatGeek*.[6] WLF filed an amicus brief in *Drummer* urging the Ninth Circuit to hold that routine IP address transmission is not a cognizable injury.[7] A ruling in defendants' favor would extend the standing framework established in *Popa* and since directly applied by district courts. On the legislative front, SB 690 remains in play as a bill that would create a "commercial business purpose" exception to CIPA's private right of action, effectively exempting commercially necessary data collection from class action exposure.[8]

---

[5] *Blaker v. NetScout Systems, Inc.*, No. 25STCV31283 (L.A. Super. Ct. May 2026).

[6] *Drummer v. CoStar Grp., Inc.*, No. 26-1160 (9th Cir. Mar 2026) (interlocutory appeal certified).

[7] *WLF Urges Ninth Circuit to Reject Privacy Claims Over Routine IP Address Transmission*, WLF Press Release, *Drummer v. CoStar Inc.* (June 4, 2026).

[8] California SB 690 (2025–2026 Reg. Sess.); *California SB 690 Advances as Two-Year Bill on CIPA Reform*, Nat'l L. Rev. (June 30, 2025).

