

Where Can Privacy Plaintiffs Sue When Injury Is Online?

By Jason Stiehl, Jacob Canter and Kari Ferver (October 29, 2024, 5:37 PM EDT)

Lawsuits against websites for allegedly spying on their users have become very common.

There are some lawsuits arising out of California, where they have been brought under a 1960s wiretapping law, otherwise known as the California Invasion of Privacy Act, or CIPA.

Pennsylvania has its own similar law, the Wiretapping and Electronic Surveillance Control Act, or WESCA. Like CIPA, a person or company found liable under Pennsylvania's wiretapping law can be subject to statutory damages of up to \$1,000 per day of the violation, as well as punitive damages, attorney fees and litigation costs.[1]

But can these lawsuits always be filed in California and Pennsylvania — even if the website owner is not located in one of these states?

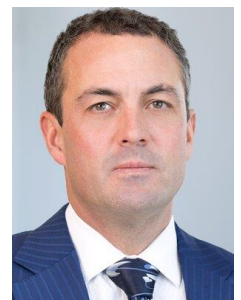
The answer is no. If the website owner is not incorporated in California or Pennsylvania, or if its principal place of business is not in California or Pennsylvania, then the website owner can only be sued in California or Pennsylvania if the court has specific jurisdiction over the website.

In September, in *Hasson v. FullStory Inc.*, [2] the U.S. Court of Appeals for the Third Circuit ruled that establishing specific jurisdiction is not as easy as 1-2-3. And in *Briskin v. Shopify Inc.*, the full U.S. Court of Appeals for the Ninth Circuit panel of judges will rule in the coming months on the reach of specific jurisdiction over a website alleged to have committed privacy violations.

Website owners need to understand these laws to understand whether they may be at risk of being sued in California or Pennsylvania courts — where the statutory damages for technical violations of half-century-old laws can be substantial. If there are ways that companies can minimize their risk without affecting their bottom line, they should take them.

Establishing Specific Jurisdiction Is Not So Simple

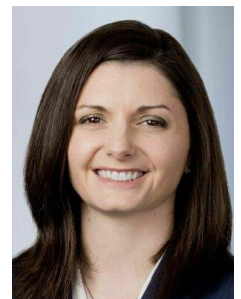
The relevant facts alleged in *Hasson* are not complex — a user visited a website. While on the website, the user's information was tracked and collected without his knowledge, and due to the anonymous tracking without his consent, he filed the lawsuit.



Jason Stiehl



Jacob Canter



Kari Ferver

In the Hasson case itself, the user sued the creator of the data-gathering code. In a companion case heard and decided alongside Hasson, the user sued the website owner, Papa Johns.

But neither FullStory nor the pizza chain are owned by a Pennsylvanian. Both companies are headquartered in Georgia and incorporated in Delaware. So, the Third Circuit asked: Does it have specific jurisdiction over these cases? Because if it doesn't, then — the Third Circuit explained — both cases must be dismissed.

The Third Circuit evaluated the dismissals under two specific jurisdictional tests: the Calder test and the traditional test. The court used both tests because, it explained, both can be applied in an intentional tort case.

The Calder test, derived from the U.S. Supreme Court's decision in *Calder v. Jones* in 1984,[3] requires a plaintiff to show that (1) the defendant committed an intentional tort, (2) the plaintiff felt the brunt of the harm from that tort in the forum and (3) the defendant "expressly aimed" its tortious activity at the forum.

The Third Circuit held that the plaintiff did not satisfy Calder's "expressly aimed" requirement. The court explained that it is not sufficient for a website to merely be accessible in a forum and for the plaintiff to allege harm there.

The plaintiff must show something more. For example, if a website is accessible in Pennsylvania and also its content "bear[s] a particular nexus to" Pennsylvania, then the expressly aimed element could be met. Or if the website had "location-specific advertisements," then the expressly aimed element could be met. Or if the website deployed code based on knowledge that it would track the data of a particular Pennsylvanian, then the expressly aimed element could be met.

It was not sufficient to just allege that the website's tracking code was intercepting someone's data, and that person happened to be in Pennsylvania. This, the court said, would not make Pennsylvania the focal point of the harmful activity so as to justify jurisdiction. The code would have wiretapped the plaintiff no matter where his computer was located, so the alleged wrongdoer did not target the state where the user was located.

This case is not the same as purchasing a physical product on a website, where the product would ultimately be shipped to the state. The injury here is entirely online, so the plaintiff needs to do more to show why the lawsuit should be filed in this particular state.

The court also looked at the allegations under the traditional specific jurisdiction test, which also has three elements.

First, a plaintiff must show that a defendant had "minimum contacts" with the forum such that it purposefully availed itself of the privilege of conducting activities there. Second, the plaintiff's claims must "arise out of or relate to" at least some of those contacts. Finally, the exercise of jurisdiction must comport with "traditional notions of fair play and substantial justice" such that the defendant should anticipate being haled into court in that forum.

The court said that under the traditional test, it was a "close call,"[4] but it still held that there was no specific jurisdiction, and the case was dismissed.

The court explained that the complaint "founders at step two" for failure to establish a strong relationship among the defendant, the forum and the litigation. The website's accessibility in Pennsylvania, by itself, was insufficient to establish this connection; the plaintiff needed to show defendants' efforts to direct Pennsylvanians to the alleged harm, such as promoting its website in Pennsylvania.

One judge in Hasson filed a concurrence/dissent. Judge Peter Phipps agreed with the majority's Calder analysis, but suggested that courts should consider recognizing a companion doctrine to Calder to "hold accountable out-of-forum data pirates." Under this theoretical doctrine, a court could find specific jurisdiction in an intentional tort case if data is captured or extracted from the forum.

But Judge Phipps disagreed with the conclusion that the traditional test was not met. He argued that the plaintiff alleged a strong "common thread" between the defendant, the forum, and the litigation — here, that the defendant chose to use its website to make pizza sales in Pennsylvania and chose to use the allegedly eavesdropping code on that website to record the plaintiff's website behavior.

To Judge Phipps, that was sufficient. To a majority of the judges on the panel, it was not.

What This Means for Website Owners That Don't Reside in Pennsylvania or California

Website owners outside of Pennsylvania should read this decision to mean that there is no guarantee that you can be sued in the fifth-most populous state, i.e., Pennsylvania.

A plaintiff can only sue you in Pennsylvania if you've done something more to aim your attention at the state. That something more may be advertisements, it may be sales in the state, it may be targeting specific Pennsylvanians. But unless Judge Phipps' "data pirates" doctrine becomes law, specific jurisdiction remains a serious hurdle for litigants seeking to file suit in Pennsylvania courts.

In fact, website owners should consider thinking more broadly about the states where they could potentially be sued.

Do you direct your advertising, both online and offline, into any specific states? Do you rely on vendors located in California, Pennsylvania or any other state? Do you share data with third parties located in another state? Do you have particularly high website traffic in any particular state? The more information you possess about your business, the more confident you can be when anticipating where lawsuits can be filed against you and a claim for jurisdiction will be accepted.

The next question on the horizon is what will happen in California — the most populous state, based on the 2020 Census — after Shopify? On Nov. 28, 2023, a three-judge panel of the Ninth Circuit held that it lacked specific jurisdiction over a similar case to Hasson, finding that the defendant's website did not expressly target California when it extracted a California website user's data.

But the circuit decided that a closer look at these facts and this law was appropriate.

Will the Ninth Circuit follow the Third Circuit and maintain that something more must be alleged than just having a website that is accessible in California? Or will the court rule in a different way, and potentially introduce a different standard for specific jurisdiction when plaintiffs allege website privacy violations?

This all remains to be seen.

Jason Stiehl is a partner, Jacob Canter is counsel and associate Kari Ferver is an associate at Crowell & Moring LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] 18 Pa.C.S. § 5701, et seq.

[2] Hasson v. FullStory Inc., 2024 WL 4049220 (3d Cir. Sept. 5, 2024).

[3] Calder v. Jones, 465 U.S. 783 (1984).

[4] Hasson, 2024 WL 4049220, at *7.