

Shopify Privacy Ruling May Spark New Wave Of Litigation

By **Abraham Gross**

Law360 (April 24, 2025, 6:18 PM EDT) -- A Ninth Circuit ruling that revived a suit alleging Shopify violated privacy laws using tracking software cleared a key procedural bar that could open the floodgates to a new wave of litigation, threatening to strain an insurance market already tested by privacy suit claims.

In its **Monday decision**, a split en banc panel found that a California federal court could hear privacy violation claims based on the company's possession of location data that placed the lead plaintiff's smartphone in the state before it when it installed tracking "cookies," seemingly lowering the jurisdictional hurdle.

The decision has the potential to add fuel to plaintiff suits based on federal law and California's relatively expansive privacy and data collection standards, which can affect several different insurance coverage lines.

"Being able to have a jurisdictional argument as one arrow in your quiver to try to get rid of the case early on is very important, and if that's taken away, then it becomes more likely that the case gets past the motion to dismiss and into the very expensive phase" said Alexander Bilus, co-chair of Saul Ewing's cybersecurity and privacy practice.

The majority found that though Shopify Inc. is based in Canada, California had jurisdiction because the company had the location data of lead plaintiff Brandon Briskin's smartphone when it installed cookies on his device.

"Applying our traditional personal jurisdiction precedent to the ever-evolving world of e-commerce, we conclude that jurisdiction is proper because Shopify's allegedly tortious actions deliberately targeted Briskin in California," Judge Wardlaw wrote for the majority.

Briskin's suit alleges the company used the data to create and sell consumer profiles to third parties without his consent, invading his privacy, illicitly collecting data without proper notice, and violating various other state and federal laws related to privacy.

These sorts of tracking and analytics cookies are incredibly common and relied upon by companies to improve their user experience and targeting of advertisement, Bilus said.

He added that in ruling that California had jurisdiction based on Shopify's knowledge of the device's location, rather than an allegation that Shopify's activities specifically targeted the state, the judges appeared to meaningfully shift its stance on jurisdictional issues, noting that the court overturned one prior decision that seemingly required targeting.

"The majority does try to suggest that it's in line with what it's done the court has done previously, but I think it is an expansion of prior principles, and they do expressly overrule one prior decision in getting there, which is a sign that they are they're doing something new here," he said.

In the past, insureds have successfully raised personal jurisdiction objections, especially when they are not located in the jurisdiction or do not purposely direct their actions there, said Matthew Bricker, founding member of TittmannWeix, which represents carriers.


"Insureds and their defense counsel have been good at getting quick dismissals where possible — for example if the plaintiff does not truly understand how the technology functions or where the insured is located," he said in an email to Law360. "But this decision appears to at minimum make that more difficult."

Unauthorized collection of data generally triggers cybersecurity policies and errors and omissions policies, while invasion of privacy claims trigger general liability and media liability coverage, according to Darren Teshima of Covington & Burling LLP.

While cyber policies are often viewed as the intuitive home for privacy-related claims, general liability policies can also offer protections under their personal and advertising injury coverages.

"These policies provide worldwide coverage, so wherever the alleged wrongful act alleged has taken place, I do think companies generally should be thinking about what coverages they have to cover these types of privacy claims wherever they are operating," Teshima said.

He also said insurers may try to argue that allegations of intentional misconduct may bar coverage, adding that plaintiffs often also allege misconduct that focuses on the unauthorized collection of data without asserting any intention on the part of the policyholder.

Jeff Kiburtz of Pillsbury Winthrop Shaw Pittman LLP told Law360 that the Ninth Circuit's decision may put substantial focus on CGL policies in light of the California Supreme Court's 2022 decision in *Yahoo Inc. v. National Union Fire Insurance Co. of Pittsburgh PA* , which appeared to expand **privacy-related coverage** under CGL policies.

There, the court ruled that commercial general liability policies may cover so-called "right-to-seclusion" violations in the Telephone Consumer Protection Act based on their coverage for injuries arising from "oral or written publication" of "material that violates a person's right of privacy."

Though the justices did not rule for coverage outright in that case, some viewed the decision — based on language taken from a standard policy form — as **significantly shifting the state** toward recognizing that CGL policies cover a broader range of privacy claims.

Assuming the Ninth Circuit decision remains law, Kiburts said that between the expansion of the kinds of cases that can be brought in California paired with the Yahoo decision, "I think you might see a lot more action under CGL policies that really focus on whether these types of claims are coming within the scope of the exclusions and those policies."

While CGL is often thought of as a last line of defense for these kinds of claims, Kiburtz said that the distinctions between professional liability, media liability and other coverages is not always clear and can be packaged differently depending on a policyholder's line of business.

"At this point, most companies are getting standalone cyber coverage, and the long-standing advice has been that you shouldn't be counting on your CGL policy to provide for what might be thought of as cyber risks, but these issues are often more challenging than insurers would like to think they are," he said.

Bricker of TittmannWeix said that coverage will depend both on the allegations of the suit and on the specific wording of the policy. Cyber policies, he noted, typically cover security events or unauthorized disclosures from bad actors while here, the issue is the company's allegedly intended use of the technology.

"Although website tracking suits are often lumped together as a broad category, there are many different technologies at issue, including cookies, session replay, tracking pixels, chatbots and other analytical tools," he said. "Policies may respond differently depending on the technology at issue."

Though policyholders may have coverage options to choose from, being subjected to California's privacy laws and subject to its jurisdiction can prove challenging in itself.

"Under our circuit's newly divined rule, when a company attaches cookies to a person's electronic device, jurisdiction attaches wherever that person happens to be, and indeed, wherever that person

happens to travel thereafter," Judge Consuelo M. Callahan said in his lone dissent that rejected the majority's "traveling cookie" reasoning.

For Bilus of Saul Ewing, the risk that the Ninth Circuit decision will incentivize plaintiffs to bring more cases or seek greater settlement amounts will push companies to consider operational changes to minimize their exposure altogether.

"I think it's a big risk for any company with a website and with cookies to not be thinking about how to best position themselves to defend against claims in California, and so potentially not being able to argue that there's no personal jurisdiction in California, I think, is a big change for those defendants," he said.

The case is Brandon Briskin v. Shopify Inc. et al., case number 22-15815, in the U.S. Court of Appeals for the Ninth Circuit.

--Additional reporting by Dorothy Atkins, Hope Patti and Shane Dilworth. Editing by Amy Rowe.

Update: This article has been updated with comment from Bricker of TittmannWeix.

All Content © 2003-2025, Portfolio Media, Inc.