LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Strain Of Web Tracking Suits Pose Risks For Retailers

By **Stephanie Sheridan, Meegan Brooks and Matthew Farrell** (January 30, 2024, 10:09 AM EST)

In the latest example of privacy laws being stretched to fit new digital technologies, plaintiffs have begun to file a flurry of suits alleging that retailers are using pen register and trap-and-trace software to illegally track website users, exposing businesses to $5,000 per violation penalties under the California Invasion of Privacy Act.

Stephanie Sheridan

Meegan Brooks

Matthew Farrell

Pen Registers and Trap-and-Trace Devices

The term "pen register" originally referred to a device — also called a telegraph register — that recorded telegraph signals on a piece of paper. At the time they were used, telegraph registers often employed a fountain pen — hence the name.

Over time, the term "pen register" came to refer to devices that recorded the number dialed on a telephone, i.e., outgoing phone numbers, while trap-and-trace devices were those that recorded the numbers that had called a telephone, i.e., incoming phone numbers.

Around the turn of the 21st century, the definition expanded once again, growing to encompass certain software programs used to track internet users' online activity, mainly in the context of government surveillance programs.

CIPA defines "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

A trap-and-trace device, defined under Section 638.50(c) of CIPA is similar, but captures incoming, rather than outgoing, signals.

This relatively expansive definition has recently been taken to the extreme by plaintiffs, who contend that any device that can track online activity and identity falls within its scope.

Plaintiffs' Newest Theory

Over the last 19 months — since the U.S. Court of Appeals for the Ninth Circuit's decision in Javier v. Assurance IQ LLC, where the court decided that a customer cannot consent to an alleged recording of their communications after the recording has already happened — plaintiffs have argued that websites engaged in wiretapping.

This includes maintaining copies of customer service chat communications, using session replay to track customers' movements across a website, and using software-as-a-service vendors to allegedly intercept such communications.

In so arguing, plaintiffs have tested several sections of the California Penal Code, including: Section 631, which addresses wiretapping; Section 632.7, which deals with eavesdropping; and Section 502,

or California's Computer Data Access And Fraud Act, a hacking prevention statute.

In the newest iteration of consumer privacy cases, plaintiffs contend that by tracking the activity of website visitors, companies violate Section 638.51 — which states that, aside from certain exceptions, "a person may not install or use a pen register or a trap-and-trace device without first obtaining a court order."

In practice, these allegations are similar to other consumer privacy claims under CIPA — including the accompanying $5,000 per violation statutory penalty — with the main difference being that Section 638.51 creates a cause of action even where no contents are recorded.

As a result, while early iterations were specifically focused on tracking Internet Protocol addresses, plaintiffs have begun to bring broader claims alleging that effectively any use of a software that may track website users can constitute a violation of the statute, which may show their high hopes for this new strain of consumer privacy cases.

Plaintiffs generally equate the use of tracking software to "create[ing] a unique digital profile of each specific website visitor," as noted in Sanchez v. National Instruments Corp. in the Superior Court of California, County of Los Angeles, in December 2023

In Greenley v. Kochava in the U.S. District Court for the Southern District of California in July 2023, U.S. District Judge Cynthia Bashant denied Kochava's motion to dismiss as to the plaintiff's Section 638.51 claim, notably stating that: The "expansive" language used in the definition of a pen register in the statute "indicates courts should focus less on the form of the data collector and more on the result" such that a process can include "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting.'"

Accordingly, the court found the plaintiff had adequately alleged that the software at issue — a software development kit developers could use to make apps, and through which the defendant was purportedly provided with geolocation, IP address and other information about app users — was a pen register.

Although the Kochava decision appears all-encompassing at first glance, it is worth noting that in Kochava, the plaintiff sued the provider of the software that allegedly tracked the plaintiff's information, not the consumer-facing party that used the software to build its platform.

Indeed, the court made clear that the issue was with the provider, not the consumer-facing party: "[I]t is Defendant's interception, packaging, and reselling of plaintiff's data that constitute the privacy violations in this case. Third-party apps are merely the vessel for Defendant's SDK [software] to collect data."

Nonetheless, the plaintiffs' bar has pointed to Kochava as opening the doors for various alleged tracking technologies — including cookies, pixels, session replay, analytics tools and more — to qualify as a pen register.

While dozens of pen register cases have been filed against e-commerce companies in the last two months, in particular, there is currently no case law other than Kochava interpreting Section 638.51 in the context of e-commerce.

However, we expect upcoming motions to dismiss to raise a number of arguments for why the statute does not actually apply, for example.

The tools at issue collect information that would take them outside the definition of pen register. Internet users have no expectation of privacy in their IP addresses — which are shared as a matter of course to allow navigation between webpages — and consent to a company's privacy policy falls within the consent exception of the statute.

How to Mitigate Risk

Especially until any more helpful case law develops, the Kochava decision will undoubtedly continue to spur more of these new suits.

Companies should review their practices to determine whether they use any technologies that could theoretically be construed as pen registers or trap-and-trace devices, taking into account what information is captured, when and if website users consent beforehand.

Additionally, companies should take steps to develop a potential argument that customers consented to any alleged uses of pen registers or trap-and-trace devices.

Section 638.51 includes an express exception where "the consent of the user of that service has been obtained." In light of this exception, businesses should evaluate whether their consumer-facing notices and consent practices are up to date, and disclose technologies that plaintiffs may contend are pen registers or trap-and-trace devices.

As the consumer privacy landscape continues to shift and evolve, remaining abreast of the latest developments is the best way for companies to minimize risk and continue to provide their customers with the seamless online experience they have come to expect.

Stephanie Sheridan is a partner and chair of the retail and e-commerce practice at Benesch Friedlander Coplan & Aronoff LLP.

Meegan Brooks is a partner at the firm.

Matthew Farrell is an associate at the firm.

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.

All Content © 2003-2024, Portfolio Media, Inc.