CLIENT ALERTS & INSIGHTS

Old Law, New Tricks: Pen Register and Trap and Trace Claims on the Rise

JANUARY 18, 2024

Authors: Matthew Farrell

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 ("CIPA").

What are 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, these devices 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." CIPA § 638.50(b). A "trap and trace" device, defined under CIPA § 638.50(c) 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 Ninth Circuit's decision in *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (May 31, 2022)), plaintiffs have argued that websites engaged in wiretapping by, e.g., 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: § 631 (which addresses wiretapping); § 632.7 (which deals with eavesdropping); and § 502 (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 CIPA § 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 § 638.51 creates a cause of action even where no "contents" are recorded. As a result, while early iterations were specifically focused on tracking IP addresses, plaintiffs have begun to bring broader claims alleging that effectively any use of a software that may "track" website users (which plaintiffs generally equate to "create[ing] a unique digital profile of each specific website visitor") can constitute a violation of the statute, which may show their high hopes for this new strain of consumer privacy cases.

In a recently decided case in California, *Greenley v. Kochava*, 2023 WL 4833466 (S.D. Cal. July 27, 2023), Judge Cynthia Bashant denied defendant Kochava's motion to dismiss as to the plaintiff's § 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*, plaintiff sued the provider of the software that allegedly tracked 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: "it 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." *Kochava*, 2023 WL 4833466, at *6. Nonetheless, the plaintiffs' bar has pointed to *Kochava* as opening the doors for various alleged tracking technologies-including, e.g., 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 § 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 which 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 notice 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.

For more information on this subject, please contact a member of Benesch's Retail & E-Commerce Practice Group.

Matthew P. Farrell at mfarrell@beneschlaw.com or 628.600.2244