February 13, 2024

California Online Tracking Lawsuits Shift Away from Wiretap Theory Toward Pen Register Theory

by Evan S. Nadel , Tatum Andres



Class-action lawyers are adapting their legal tactics, moving away from suing companies under California's wiretap law and instead focusing on a new legal claim: the pen register theory.

For the past two years, website owners that gather data from California residents have faced a surge in class action lawsuits and threatened lawsuits alleging violations of the California Invasion of Privacy Act (CIPA). These lawsuits assert that the use of web analytic tools such as session replay, chatbots, and tracking pixels constitute a violation of CIPA's wiretapping provisions. Specifically, Section 631(a) of the CIPA prohibits third parties from engaging in unauthorized wiretapping or eavesdropping on a communication between two parties. However, in 2023, California courts began regularly dismissing these state wiretap claims for various reasons. Some courts ruled that the plaintiffs failed to demonstrate concrete harm or injury resulting from the alleged recording of their interactions. Other courts found that the plaintiffs lacked standing because they could not establish that the contents of their communications were intercepted or accessed by third parties.

In light of these dismissals, plaintiffs' attorneys hope that they'll find more success bringing cases under Section 638.51 of CIPA, California's pen-register law, which is broader than the wiretap statute and does not contain the same hurdles.

Pen registers have a long history (pre-internet) as physical, real-world crime fighting devices used to track all outgoing phone numbers called from a particular telephone line. Installation of pen registers to record a specific phone line was banned by statute and required law enforcement to apply for and obtain a court order. Moving to the internet era, plaintiffs now claim as part of a new theory of liability that modern web tracking tools such as cookies, web beacons, pixels, scripts, or software code, to monitor a user's location, search queries, browsing activity, or purchase history, are the functional equivalent of the pen register, and that without a court order, use of these technologies violates the same statute that bans pen registers.

Companies concerned about exposure stemming from their use of user-tracking software should note that while the legal theory may differ, the best way to mitigate risk remains the same: obtain affirmative user consent prior to deploying any user-tracking software.

The Rise of Pen Register Litigation: *Greenley v. Kochava*

CIPA allows any person to bring a private right of action for an injunction as well $5,000 per violation or treble damages, whichever is greater. Under the wiretap statute, plaintiffs had to show that monitoring software was deployed without consent *and* that the software captured communications.[1] Under the pen-register statute, however, plaintiffs do not have to show that the contents of any communications were recorded. Instead, all they have to show is that a pen register was deployed without user consent.

CIPA prohibits the installation of pen registers without consent or a court order.[2] CIPA defines a 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."[3]

The latest wave of litigation directly challenges the ability of website owners to use modern internet technologies, including tracking pixels, chatbots, and session replay, asserting that these technologies constitute a "pen register" that has been illegally installed.

Greenley v. Kochava is a 2023 case from the U.S. District Court for the Southern District of California that provided the launching pad for this theory. In *Greenley*, the plaintiff accused a data broker, Kochava, Inc., of using a software development kit to collect user data and sell it to third parties. Specifically, the software development kit, which was used in various smartphone apps, was able to track the user's geolocation, purchase decisions and payment methods. With this information, Greenley alleged that Kochava was able to deliver targeted advertising based on the users' locations, spending habits, and personal characteristics.

In order to avoid liability, Kochava argued that the software development kit did not constitute a "pen register," which historically was a physical device used to track the phone numbers dialed on a telephone's outgoing calls. In ruling on Kochava's motion to dismiss, the Court rejected this argument. It held that, today, pen registers can take the form of software. In fact, due to the expansive language the California legislature chose in defining "pen register," courts should focus less on the form of the data collector and more on the result.

This definition is problematic, even for companies who take proactive steps to ensure compliance with CIPA. A broad definition of a pen register leaves the door open for virtually any device that collects data to constitute a pen register, even a smartphone. In light of the *Greenley* decision and statutes similar to CIPA in other states, website owners should anticipate the filing of more pen register lawsuits in the near future.

Plaintiffs' attorneys are also starting to send demand letters alleging violations of the related "trap and trace" provision of CIPA: rather than track data from outgoing communications like a pen register, a trap and trace device captures "the *incoming* electronic or other impulses that identify the originating number or … other signaling information reasonably likely to identify the source of a wire or electronic communication."[4]

So What Happens Now?

As with any new legal theory, it will take time for the case law to develop. However, we know that Section 638.51 allows for the use of pen registers where the consent of the user has been obtained. Additionally, under

California Penal Code 502(j), “a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.” Therefore, if an individual is in California when a non-California website owner accesses the individual's device, the website owner will be subject to jurisdiction in California.

So, in the meantime, companies that operate websites that individuals in California can access should focus on three main action items:

1. Ensure that your website has a cookie banner that discloses the use of user-tracking software. Tracking software should not be deployed until the user affirmatively consents to its use by clicking “accept” on the cookie banner.
2. Disclose the use of user-tracking software in your privacy policy. Be transparent about what software is used, what it records, and what types of third parties the data may be shared with.
3. Ensure that you maintain a record of the consent mechanism to be able to prove, at a later date, that a user would not have been able to access your website without accepting your cookie banner.