FEBRUARY 29, 2024

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

by Evan S. Nadel , Tatum Andres

For the past several 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 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. Following these dismissals, some attorneys challenging online tracking have pivoted to Section 638.51 of CIPA, California's "pen-register" law, which is arguably broader than the wiretap statute.

Pen registers have a long (pre-internet) history 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. *Id.* § 638.51. Some plaintiffs' attorneys have begun to claim 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 constitute the functional equivalent of a pen register. Under this theory, the use of these technologies without a court order violates the statute that bans physical 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 before deploying any user-tracking software.

The *Greenley v. Kochava* decision denied a motion to dismiss a "pen register" claim

CIPA allows any person to bring a private right of action for an injunction, as well as $5,000 per violation or treble actual damages, whichever is greater. Under the wiretap statute, plaintiffs must show that monitoring software was deployed without consent *and* that the software captured communications.

Cal. Penal Code § 631. Under the pen register statute, however, plaintiffs do not have to show that the contents of any communications actually were recorded—only that a pen register was deployed without user consent.

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." *Id.* § 638.50(b). Some recent cases challenge the ability of website owners to use modern internet technologies such as tracking pixels, chatbots, and session replay under the theory that these technologies constitute a "pen register" that has been illegally installed.

In *Greenley v. Kochava, Inc.*, --- F. Supp. ----, No. 22-cv-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023), the plaintiff accused a data broker (Kochava) 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.

To avoid liability, Kochava argued that the software development kit did not constitute a "pen register," which (as noted above) historically was viewed as a physical device used to track the phone numbers dialed on a telephone's outgoing calls. Denying Kochava's motion to dismiss, the court held that pen registers can take the form of software and that, in light of 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.
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.

Some class action plaintiffs' attorneys have also sent 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." Cal. Penal Code § 638.50(c).

Even non-California website operators must be mindful of possible pen register claims. 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.

Action Items to Mitigate the Risk of Pen Register Claims

Section 638.51 of CIPA allows for the use of pen registers where the consent of the user has been obtained, so securing consent is the best proactive measure against pen register claims. Companies that operate websites that individuals in California can access should focus on three main action items. First, 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. Second, 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. Third, ensure that you maintain a record of the consent mechanism to be able to prove that a user would not have been able to access your website without accepting your cookie banner.