PEN REGISTER AND TRAP AND TRACE CLAIMS: THE LATEST WAVE OF CIPA LITIGATION

Date: 4 March 2024

US Litigation and Dispute Resolution Alert

By: Michael J. Stortz

A new species of website privacy litigation has taken hold in 2024, based on arcane provisions of the California Invasion of Privacy Act (CIPA) that restrict law enforcement's use of pen register or trap and trace devices without a court order. Scores of class action and individual lawsuits have been filed asserting the novel theory that common website technology, including web beacons and pixels, run afoul of these provisions, which traditionally have been limited to physical devices that record the numbers dialed from a specific telephone line, or the originating numbers of calls placed to the line.

Even though the lawsuits are in the early stages, some likely defenses and risk-mitigation strategies have begun to emerge. We review the core claims and initial rulings and then consider likely defenses and steps that companies might consider in response to this latest variation of CIPA claims.

BACKGROUND

In recent years, an onslaught of CIPA litigation has inundated the California federal and state courts claiming that different website technologies, ranging from session replay software to chatbots to pixel tools, violate the anti-wiretapping provisions of CIPA. Plaintiffs have achieved mixed results, as defenses to the claims—including consent and lack of injury—often resulted in favorable outcomes for defendants. In addition, courts grew increasingly skeptical of the bona fides of some of the cookie-cutter lawsuits otherwise presented as legitimate class action complaints.

Plaintiffs have now latched onto a new CIPA theory based on an unpublished 2023 trial court decision, *Greenley v. Kochava*,[1] which addressed the application of the pen register provisions of CIPA to defendants' software developer kits (SDKs). Plaintiff claimed that defendant's SDKs secretly collected multiple types of data from upstream app users, which defendant in turn used to “fingerprint” each user, and to sell the resulting user profiles to third parties. In addition to multiple other claims under federal and state law, plaintiff claimed that defendant's SDK violated CIPA Section 638.51's prohibition against the installation or use of a pen register without a court order.

Ruling on defendant's motion to dismiss, the court rejected defendant's narrow argument that CIPA's pen register provision is limited to physical machines appended to traditional phone lines. The court reasoned that, given the “vague and inclusive” statutory definition, a pen register might include software “that identifies consumers, gathers data, and correlates that data through unique fingerprinting,” as defendant's SDK allegedly did. The court did not consider whether website hosts, as opposed to third-party interlopers, could be liable under these provisions for implementing tools such as session replay software and pixels on the host's own website.

©2005-2026 K&L Gates LLP. All Rights Reserved.

LITIGATION ISSUES

Even so, certain segments of the plaintiffs' bar have invoked the *Greenley* decision to launch a new wave of litigation, claiming that online analytical or tracking tools amount to pen registers or trap and trace software subject to the CIPA. The result has been a tsunami of lawsuits and demand letters, with one firm filing over 120 lawsuits on this claim in recent months.

A basic defect in these claims is that CIPA's pen register restrictions cannot plausibly be interpreted as applying to website sponsors and other intended recipients of online communications, as opposed to third-party SDKs at issue in *Greenley*. Identical provisions in the federal pen register statute have been construed by federal courts as not applying to the recording of IP addresses since routine Internet functions require recording of IP addresses so that users can communicate with each other.

CIPA's compliance provisions also contradict these lawsuits' core premise that consumer-facing website technologies can be fairly construed as pen registers or trap and trace devices. CIPA limits the use of such devices to specific law enforcement purposes and requires that an order approving their use specify “the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached” and the identity “of the person who is the subject of the criminal investigation.” Cal. Penal Code § 638.52(d)(1)-(3). By contrast, the website technology challenged in the recent wave of “pen register” litigation involves website technology that is user-agnostic and cannot be approved for use only as to a specific person or particular telephone line.

RISK-MITIGATION OPTIONS

As the *Greenley* court recognized, until the recent wave of CIPA litigation, no court had previously interpreted CIPA's pen register provisions. As such, the scope of the statute, and whether it extends as broadly as plaintiffs claim, remains to be determined. While courts analyze these questions, companies might consider several factors in evaluating this latest litigation wave.

At the threshold, the scope of these CIPA claims may be limited to California-based companies, given the presumption against extraterritorial application of California statutes such as CIPA for activity that occurs outside of the state. In addition, out-of-state companies may not be subject to litigation in California based on the out-of-state conduct that purportedly gives rise to these claims.

For California-based companies, the core defenses to CIPA anti-wiretapping claims likely apply to these CIPA pen register claims. User notice and disclosures in online privacy statements are expected to provide robust defenses to the claims, with the effectiveness of such notice and disclosure likely to be evaluated under the same standards that apply to CIPA claims and data privacy claims more broadly. The lack of any actual injury resulting from use of these technologies also will provide a critical litigation defense. Arbitration and class waiver provisions also may provide a bulwark against litigation.

As we continue to see the results of increased judicial scrutiny on this slew of litigation, we expect the coming months to yield much-needed clarity around the legitimacy of these claims. In the meantime, companies may already have developed substantial defenses to any litigation through prior compliance efforts.

©2005-2026 K&L Gates LLP. All Rights Reserved.

FOOTNOTES

[1] No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

KEY CONTACTS



MICHAEL J. STORTZ
PARTNER

SAN FRANCISCO
+1.415.882.8011
MICHAEL.STORTZ@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.