Cos. Should Mind Website Tech As CIPA Suits Keep Piling Up

By **Wynter Deagle, Anne-Marie Dao and Teresa Morin** (April 12, 2024)

Wynter Deagle

Anne-Marie Dao

Teresa Morin

Over the last two years, the landscape of privacy litigation evolved significantly as plaintiffs sought to stretch the decades-old California Invasion of Privacy Act to accommodate novel legal theories based on businesses' use of commonplace website technologies. That evolution has continued apace in 2024.

Since late December 2023, a certain component of the plaintiffs bar has inundated businesses with demand letters, individual lawsuits, and purported class actions alleging a new theory of CIPA liability based on the use of website technologies — violation of the provisions that restrict the use of a pen register or a trap-and-trace device without a court order.

The number of these demands and lawsuits has increased exponentially in 2024.

Stalking Pixels: Plaintiffs' Counsel Transform Into Web Technology Detectives

The original deluge of CIPA litigation was triggered in 2023 by Javier v. Assurance IQ LLC, a U.S. Court of Appeals for the Ninth Circuit unpublished decision that held that CIPA "applies to Internet communications."[1]

Relying on that decision, plaintiffs firms scoured the web for businesses using web technologies and issued hundreds of presuit demand letters based on claims that the use of various website technologies violated the anti-wiretapping provisions of CIPA[2]. Class actions on behalf of professional litigation testers soon followed.

The liability theories initially advanced fell into three general buckets: (1) that chatbots managed by third-party vendors illegally intercepted the contents of consumer communications; (2) that the website technology was an illicit and unannounced eavesdropper; or (3) that the web technology constituted doxing because it revealed the identity of anonymous consumers.

These claims challenged the legality of a wide range of website technologies including session replay software, heat mapping software, chatbots, cookies, web beacons and pixels.

Many businesses chose to settle claims and cases early and on an individual basis to avoid the expense of litigation. The lawsuits themselves, however, were subsequently met with mixed results. Many website operators mounted successful defenses based on consent that the web technology vendor was a party to the communication, lack of standing and lack of injury.

In addition, courts also increasingly looked askance at cookie-cutter lawsuits brought by serial litigants who were self-titled "litigation testers."

The Pen Register and Trap-and-Trace Provisions Dial Up Trouble

CIPA itself, however, remained an attractive litigation for plaintiffs because the statute includes statutory damages of $5,000 per violation. As wiretapping started petering out, an arcane, and little noticed, provision of CIPA provided a new basis for plaintiffs to continue their pursuit of CIPA's statutory damages.

Section 638.51 of CIPA prohibits the installation or use of a pen register or a trap-and-trace device without first obtaining a court order. Unlike a wiretap, which permits interception of the content of the communications, pen registers and trap-and-trace devices are limited to the collection of dialing, routing, addressing or signaling, or DRAS, information.

Specifically, a pen register is defined as "a device or process" that records or decodes DRAS information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."[3] Similarly, a trap and trace is defined as "a device or process that captures the incoming electronic or other impulses that identify" the DRAS or originating number "reasonably likely to identify the source of a wire or electronic communication."

An unpublished 2023 decision from the U.S. District Court for the Southern District of California[4] was the first to pit CIPA Section 638.51 against web technologies. In Greenley v. Kochava, the plaintiff claimed that the defendant Kochava's software development kits, or SDKs, secretly collected multiple types of data from the users of third-party mobile applications.

The plaintiff alleged that Kochava used the data to "fingerprint" each user and to sell the user profiles created from the data to other third parties. In addition to multiple other state and federal law claims, the plaintiff contended that the Kochava's SDK violated CIPA Section 638.51's prohibition against the installation or use of a pen register without a court order.

In response, Kochava filed a motion to dismiss arguing that the SDK was not, as a matter of law, a pen register. Judge Cynthia Bashant denied the motion as to the Section 638.51 claims.

As an initial matter, Judge Bashant held that while pen registers had traditionally been physical machines used by law enforcement agencies "to record all numbers called from a particular telephone," such pen registers now "take the form of software."[5] She further noted that by using such software, "private companies and persons have the ability to hack into a person's telephone and gather the same information as law enforcement" and speculated that "[p]erhaps for this reason, the California legislature does not limit its prohibition on installing pen registers to law enforcement."[6]

Bashant then turned to the "expansive language in the California Legislature's chosen definition" for pen register. After noting that no other court had interpreted CIPA's pen register provision, the court articulated that the definition was specific as to the type of data a pen register collects — DRAS information — but "vague and inclusive as to the form of the collection tool — 'a device or process.'"[7]

The court concluded that the language suggests that "courts should focus less on the form of the data collector and more on the result."[8]

Accordingly, Bashant applied the plain meaning of a process to the statute, and concluded that a process may include software "that identifies consumers, gathers data, and correlates

that data through unique fingerprinting," as defendant's SDK allegedly did.[9] On that basis, Bashant rejected Kochava's "contention that a private company's surreptitiously embedded software installed in a telephone cannot constitute a 'pen register.'"[10]

And Away We Go…

Importantly, Bashant's ruling in Greenley did not address whether a business that operates a website, as opposed to third-party technology providers, could be liable for violations of CIPA's pen register and trap-and-trace device provisions for implementing website technology such as pixels on their own website.

Undeterred, however, following the Greenley decision, a certain component of the plaintiffs bar invoked Greenley as a new basis for CIPA violations based on the use of website technologies. The result has been another surge of demand letters, largely sent by the same lawyers on behalf of the same litigation testers who were behind the original wave of CIPA demands.

And many of the demand letters have been sent to the same businesses that previously settled CIPA claims with these same firms or plaintiffs. In addition, two of these firms have collectively filed over 150 lawsuits in California state courts alleging violation of CIPA Section 638.51, arguing that website technologies were either pen registers or trap-and-trace devices.

The latest round of CIPA claims are in their infancy. To date, there has been no clarity from the courts regarding the scope of the statute and whether it broadly extends to the use of website technology on a business's own website.

Risk Assessment and Mitigation

Importantly, Section 638.51 allows "a provider of electronic or wire communication service" to use a pen register or trap-and-trace device "[i]f the consent of the user of that service has been obtained."

Though no court has yet applied this provision to the current round of claims, a user's affirmative consent has been fatal to other CIPA claims. Accordingly, businesses should continue to evaluate their use of website technology and other software to gather data and review the disclosures in their privacy policy to strengthen their ability to establish affirmative consent.

Wynter L. Deagle is a partner, and Anne-Marie Dao and Teresa Morin are associates, at Sheppard Mullin Richter & Hampton LLP.

[1] Javier v. Assurance IQ LLC, No. 20-CV-02860-CRB, 2023 WL 3933070 (N.D. Cal. June 9, 2023).

[2] Cal. Civ. Code §§ 631(a) and 632.7.

[3] Cal. Civ. Code § 638.50(b).

[4] Greenley v. Kochava, Case No. 22-cv-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

[5] Id. at *15.

[6] Id.

[7] Id.

[8] Id.

[9] Id.

[10] Id.