LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Kochava Ruling May Hint At Next Privacy Class Action Wave

By **Jason Stiehl, Jacob Canter and Rashmi Shivnani** (November 27, 2023, 5:32 PM EST)


Jason Stiehl


Jacob Canter


Rashmi Shivnani

Over the last year, plaintiffs have introduced new theories for civil liability under the California Invasion of Privacy Act.

These include complaints alleging that online targeted advertising technology reveals the identity of anonymous consumers,[1] that pixel-tracking technology illegally wiretaps website consumers, and that website chatbots managed by third-party vendors are illicitly spying on the contents of consumer communications.[2]

The new wave of privacy litigation may be upon us — complaints alleging that a consumer website is an illegal "pen register" due to the use of certain third-party marketing software tools, causing the website to violate the California Invasion of Privacy Act, another sub-provision of Section 638.51 of the California Penal Code.[3]

This new theory of civil liability is another example of plaintiffs challenging the use of common website marketing tools. It is important for website owners to proactively confirm whether they are using these tools through their websites.

If so, they should take affirmative steps to confirm there is no risk if served with a class action complaint.

Pen Register

CIPA was enacted in 1967 as part of the penal code to protect the rights of Californians to have private conversations free from eavesdropping devices.

Section 638.51 prohibits use of a pen register or a trap-and-trace device without a court order.[4]

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.[5]

A common example of a pen register is a device on a computer that records a list of e-mail addresses contacted. A trap-and-trace device refers to a device or process that captures the information that identifies the originating number or other DRAS information reasonably likely to identify the source of a

wire or electronic communication.[6]

A common example of a trap-and-trace device is a device in a cell phone that makes a log of incoming phone numbers.

While CIPA generally prohibits the use of a pen register or trap-and-trace device without a court order, there are limited exceptions — for example, where a service provider's customer consents to the device's use, or to protect the rights of a service provider's property.[7]

CIPA allows any person to bring a private right of action for an injunction. Also under CIPA, successful plaintiffs are entitled to the greater of $5,000 per violation or treble damages.[8]

Greenley v. Kochava: Liability Under Section 638.51

In Greenley v. Kochava Inc. in July, the U.S. District Court for the Southern District of California denied the portion of the defendant's motion to dismiss aimed at the plaintiff's Section 638.51 claim.[9]

Kochava develops code that helps software developers build their own phone applications.
The complaint alleges that Kochava built software for its clients and, in return, was granted permission to intercept the location data for the clients' application users.

Kochava then allegedly sold that data to third parties. The complaint alleges that the plaintiff's use of the apps that contain Kochava software provided Kochava with the plaintiff's personal information, geolocation data and communications.[10]

Kochava argued that users like the plaintiff consented to its access to and use of their data in two ways. First, they consented to sharing their location with a third-party app developer when they downloaded the application, and second, they failed to opt out by contacting Kochava and requesting data deletion.

The court found that neither argument shows that the plaintiff consented to Kochava's use and disclosures of data.[11]

The court reasoned that as consent is limited to the conduct authorized, the plaintiff's consent to app developers to collect data does not allow Kochava to intercept the plaintiff's data or disclose that data. Kochava's second argument also failed because the plaintiff was not aware of Kochava's activities, let alone Kochava's policies regarding opting-out of data disclosure practices.[12]

As Kochava failed to show that the plaintiff consented to its data practices, Kochava was unable to benefit from the consent exception carved out under Section 638.51.[13]

The court also disagreed with Kochava that a CIPA violation requires identifying a specific communication that was intercepted. At the motion to dismiss stage, the court reasoned that such "an inference is reasonable given the detailed allegations of the defendant's practices and the plaintiff's" use of apps installed with Kochava's software.[14]

And finally, Kochava argued that its software is not a pen register. The court disagreed.

It held that "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting'" qualifies as a "pen register." The court rejected "the contention that a private

company's surreptitiously embedded software installed in a telephone cannot constitute a 'pen register.'"[15]

The court stated that the definition of pen register is not limited to a device, but also includes any process that records or decodes dialing, routing, addressing and signaling information, thus expanding the scope of what can qualify as a pen register.

The court here observed that the California Legislature had chosen "expansive language," and "the court cannot ignore" such language.[16]

New Cases and the Road Ahead

A growing number of cases seek to hold responsible online retailers who have deployed software on their websites to allegedly identify the internet protocol addresses of the websites' visitors, and consequently, other personal identifiers about the visitors.

The plaintiffs in these cases argue that the software on these websites qualify as pen registers under CIPA, and that the defendants use this software to access and install tracking code on the plaintiffs' devices.

As we have seen previously, this is an effort to build upon the expansive language in California's privacy statutes and to apply these statutes to new technologies that did not exist when CIPA was first enacted in 1967.

If other courts follow the Greenley court's view that they cannot ignore the expansive language, then we should anticipate more and more cases filed under CIPA being applied to more and more different software applications.

The ruling in Greenley may just be the beginning. We have observed several recent filings of cases based upon the logic of Greenley in the California Superior Court.

Notably, these cases are industry agnostic — they target anyone with a variety of alleged pen registers running in the background of the website.

Thus, website owners should assess what data-tracking software they use on their websites and determine, on an application-by-application basis, whether proactive steps can, and should, be taken to mitigate the liability risks.

Jason Stiehl is a partner, and Jacob Canter and Rashmi Shivnani are associates, at Crowell & Moring LLP.

[1] Jason Stiehl et al., Another Wave of California Privacy Suits—Deanonymization as "Doxing", Crowell & Moring LLP (Aug. 8, 2023), https://www.crowell.com/en/insights/client-alerts/another-wave-of-california-privacy-suitsdeanonymization-as-doxing.

[2] Jason Stiehl et al., Chatbot Lawsuits Push Calif. Courts To Rethink Wiretap Law, Law360 (Sept. 11, 2023, 1:55 PM), https://www.law360.com/articles/1718629/chatbot-lawsuits-push-calif-courts-to-rethink-wiretap-law.

[3] Cal. Penal Code § 638.51.

[4] Id.

[5] Cal. Penal Code § 638.50(b).

[6] Cal. Penal Code § 638.50(c).

[7] Cal. Penal Code § 638.51(b).

[8] Cal. Penal Code § 637.2.

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

[10] Id. at *1.

[11] Id. at *5.

[12] Id.

[13] See Cal. Penal Code § 638.51(b).

[14] Id. at *14.

[15] Id. at *15.

[16] Id.