Coblentz
Patch Duffy
& Bass LLP

You've Worked To Make Your Website Cookies, Pixels, and Chat Function Compliant With Privacy Laws; Now What Is A "Pen Register"?

Key Takeaways

- Despite your recent efforts to comply with privacy law requirements for website cookies, pixels, and analytics, your business may be at risk of getting sued for violations of "pen register" or "trap and trace" laws based on information collected from website or mobile app users.
- A recent court decision has breathed new life into pen register and trap and trace claims. More than 75 complaints have been filed in California courts the past few months, and courts addressing these claims will need to reconcile the clear inconsistency between older pen register laws and more recent data privacy laws such as the EU's GDPR and California's CCPA/CPRA.
- Businesses should be aware of what cookies, analytics, and other website technologies they are running on their websites.

In the world of data privacy litigation, plaintiffs' attorneys are always looking for the next big thing. Over the past couple of years, plaintiffs in California and elsewhere have tried to use decades-old wiretapping and eavesdropping statutes against companies, claiming that the use of website chat functions, session recording tools, cookies, pixels, and other tracking software amounted to "wiretapping" or "eavesdropping" on website visitors.

Having found limited success with these legal claims, the newest tactic in privacy litigation appears to rely on the theory that website cookies or other website analytics tools constitute "pen registers" or "trap and trace" devices under the California Invasion of Privacy Act ("CIPA"), California Penal Code § 638.51. The basis for these new claims appears to stem from a single recent decision, *Greenley v. Kochava*, 22-cv-01327-BAS-HSG, — F.Supp.3d —-, 2023 WL 4833466 (S.D. Cal. July 27, 2023) ("*Kochava*"), where the court – acknowledging that it was an issue of first impression[1] – allowed pen register claims to move beyond the motion to dismiss stage, at least in the context of that case. *Kochava* has opened the floodgates to pen register litigation, as over 75 complaints have been filed in California courts over just the past couple of months, asserting vague and formulaic violations of pen register laws, with many more cases likely to follow.

So, what is a "pen register"? Explaining the term requires remembering a time before the Internet and cellular telephones when special equipment was necessary to record numbers dialed to or from a landline telephone. Historically, pen registers were devices that could record numbers dialed to or from a particular telephone and were often used in criminal investigations. Laws prohibiting the use of pen registers without consent or a warrant were targeted at eliminating conduct akin to surveillance done under the color of law without proper authorization.[2] The federal pen register statute, passed in 1986, did not contemplate a world where cellular phones are ubiquitous portable handheld computer devices that now identify and record all phone numbers dialed to and from them, let alone application of the law to the Internet, where identification of computers and routers through IP addresses and other electronic source information is necessary to all website interactions. And, while the 2001 USA Patriot Act and certain state laws expanded the definition of a pen register to try to address computer and Internet communications, these laws were still largely based on older statutory language and definitions that are not a precise or comprehensive fit for all of the various electronic communications and interactions that occur online or through mobile devices today.

Returning to the present day, up to and until the *Kochava* case, there has been little to no civil litigation over the use of pen registers.[3] As noted above, there are good reasons for this. Cellular telephone technology, the Internet, and other advances have changed how we communicate. The pen register statutes apply, if at all, awkwardly to advancing technologies, and there are newer privacy laws specifically aimed at Internet privacy. However, because California's pen register law 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, plaintiffs in *Kochava* sought to dust off the pen register law to apply it to Internet communications. In *Kochava*, plaintiffs asserted violations of the pen register law against a data broker company that provided a software development kit ("SDK") to application developers. As the *Kochava* court noted, application-based companies could then embed Kochava's SDK in their mobile applications to

> 'deliver targeted advertising . . . by in essence 'fingerprinting' each unique device and user, as well as connecting users across devices and devices across users.' The data links longitude and latitude coordinates with these fingerprints, which can be 'easily de-anonymized.' In addition to geolocation, [the SDK allows apps] to 'search terms, click choices, purchase decisions and/or payment methods.' This data collection allows [Kochava to] deliver 'targeted advertising . . . while tracking [users'] locations, spending habits, and personal characteristics' and share this 'rich personal data simultaneously with untold numbers of third-party companies.'

Kochava, 2023 WL 4833466, at *2-3 (internal citations to complaint omitted). Given this unique software and its purported ability to collect a treasure trove of information that could create a personal unique identifier, the *Kochava* court held that the SDK at issue amounted to a "process" that could collect "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." *Id.* at *27. Thus, *Kochava* "reject[ed] the contention that a private company's surreptitiously embedded software installed in a telephone cannot constitute a 'pen register'" and allowed the claim to proceed past the motion to dismiss stage.

For now, it is unclear how broadly or narrowly courts will apply *Kochava*. *Kochava* involved a data broker with particular software used on mobile applications. The Kochava court carefully parsed through the "pen register" statute to conclude that "software installed in a telephone" could constitute a "pen register." Accordingly, the *Kochava* holding merely stands for the proposition that a pen register claim may proceed (but not necessarily succeed) against a data broker (an entity selling data for targeted advertising rather than simply collecting it for its purposes) that installed software on users' telephones (as opposed to on websites), purportedly without consent. It would seem to require a broad leap for other courts to apply this holding generally to find that the mere collection of data through website cookies or analytics that facilitate online interactions and transactions with consumers – and which is necessary for website operations and done by every company that operates a website – violates the law. Such a holding would essentially cripple online commerce and all other Internet communications and activities.

While the *Kochava* decision may have breathed new life into pen register and trap and trace theories for the moment, courts addressing these claims must confront and reconcile the clear inconsistency between older pen register laws and more recent data privacy statutes that specifically govern the processes and disclosures companies must use when collecting consumer information on their websites, including via cookies and other analytics.

For example, the European Union's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), and many other state privacy laws all carefully and explicitly regulate how personal information may be collected from individuals, including on Internet websites. These statutes emphasize transparency and disclosure of data collection practices through privacy notices, cookie banners, and other just-in-time methods, which allow consumers to exercise their privacy rights and control the flow of information transmitted on the Internet. But even if companies are compliant with these more recent privacy laws, they may be found to violate the old pen register and trap and trace laws if applied broadly and extended to Internet technologies. This is because, taken broadly, every company in the world that operates a website necessarily collects certain device source information in connection with website interactions. Yet, avoiding the collection of such information in the context of the Internet – an ecosystem of connected computers – is impossible. Thus, it remains to be seen whether courts will find that every company is violating the law by participating in online commerce, even when (or especially when) they are complying with more recent privacy laws that specifically regulate how companies collect and process the precise information at issue in these new pen register cases.

For now, plaintiffs' attorneys will use *Kochava* as a foothold in an attempt to expand the pen register statute and expand *Kochava*'s fact-specific holding. Until courts consistently determine how to apply the pen register laws, if at all, to Internet communications, and reconcile such laws and claims against the backdrop of recently enacted privacy laws, we will all be riding this new wave of privacy litigation together.

Please contact the Coblentz Data Privacy Team with questions or to assist with any privacy claims or needs.

Authors

Scott C. Hall

Partner
San Francisco

Details
415.772.5798
shall@coblentzlaw.com

Amber Leong

Associate
San Francisco

Details
415.268.0535
aleong@coblentzlaw.com

[1] And in fact, *Kochava* was the first case to ever cite to the California pen register statute, and at the date of this publication, still the only case to have cited to and analyzed the provision.
[2] Notably, the United States Supreme Court has held that individuals do not have a reasonable expectation of privacy under the Fourth Amendment of the U.S. Constitution to suppress any evidence obtained from pen registers. *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (noting that a pen register has "limited capabilities" and the petitioner had no "legitimate expectation of privacy" regarding the numbers he dialed).
[3] To the extent the litigation was not derivative of any criminal charges.