CLIENT ALERT

NEAL GERBER EISENBERG

Navigating the CIPA Landscape: Understanding Tracking Technology Litigation and Compliance Strategies

By: Kate Campbell, Alfred Tam, David Wheeler & Josh Hanson

July 23 , 2024

Last year saw a flurry of website tracking technology litigation sparked by a broad interpretation of invasion of privacy laws that were not originally intended to apply to online technologies. Unfortunately, hopes of clarity through legislation or court decisions have not been realized. Companies remain exposed to potential class action claims and other demands related to their use of cookies, pixel tags (web bugs), web beacons, session replay software, third-party chatbots, or other tools that track user engagement on websites ("Tracking Technologies"). These lawsuits claim that the use of Tracking Technologies violates states' invasion of privacy statutes, most commonly the California Invasion of Privacy Act ("CIPA").

What are Pixel Tags and How Do They Work

A tracking pixel (also known as a web beacon or pixel tag) is a one-pixel image that is so small that it is undetectable by website users. The use of a pixel tag is currently the most common basis for a CIPA claim. This type of Tracking Technology has been used across the web-based digital ecosystem since the late 90s. Website programmers embed pixel images into webpages, chatbots, information forms, email, and online ads by companies and their third-party analytics providers. These third-party companies generally use the code associated with the image to track user behavior. In most cases, pixel technology captures information, including browser type, operating system version, IP address, time, geolocation, device details, and more. But other forms of Tracking Technologies allow third parties to directly collect user information, and such collection may violate laws such as the CIPA, where user consent is required.

California Invasion of Privacy Act Claims

CIPA prohibits "wiretapping" without both parties' consent and prohibits the use of a "pen register" or "trap and trace device" without consent or a court order. CIPA creates a private right of action and imposes statutory penalties of $5,000 per violation plus attorney's fees, making it an attractive cause of action for plaintiffs' lawyers. "Wiretapping" is defined in CIPA as using a machine or instrument to intentionally make a connection via a line or cable to read or attempt to read the contents of a communication. A "pen register" is a device or process that records the dialing, routing, or signaling that information is being transmitted but not the contents of that transmission). Similarly, a "trap and trace device" is a device or process that captures incoming electronic or other impulses that identify the originating number or dialing, routing, or signaling information that will reasonably likely identify the source of the wire or electronic communication, but not its contents. Plaintiffs claim in these shakedown suits that the use of Tracking Technologies on a website without consent amounts to wiretapping or unauthorized use of a pen register or trap and trace device.

The Current State of CIPA Litigation

The influx of CIPA litigation began with an unpublished decision by the Ninth Circuit Court of Appeals in *Javier v. Assurance IQ, LLC*, in which the Ninth Circuit held that CIPA "applies to Internet communications" and that plaintiff had properly stated a claim that defendant's use of session replay technology on defendant's website without plaintiff's consent violated the wiretapping provisions of CIPA. Over a year later, the Southern District of California offered another legal theory for CIPA violations and held that "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting' is a process that falls within CIPA's pen register definition." The controversially broad interpretation of what constitutes a "pen register" has opened the door for the recent onslaught of CIPA litigation many companies now face.

[1] Cal. Penal Code § 630, et seq.
[2] *Id*. at § 637
[3] *Id*. at § 631.
[4] *Id*. at § 638.50(b)

Legal experts have been watching for a decision that would offer some respite for companies defending what many consider "troll" lawsuits. In March of this year, the Superior Court of Los Angeles offered that glimmer of hope by agreeing that online devices that record IP addresses cannot be pen registers, finding that "nothing in the complaint establishes an IP address as equivalent to the 'unique fingerprinting' relied upon by the Southern District." The court offered a strong rebuke to the Southern District's interpretation: "[P]ublic policy strongly disputes Plaintiff's potential interpretation of privacy laws as one rendering every single entity voluntarily visited by a potential plaintiff, thereby providing an IP address for purposes of connecting the website, as a violator. Such a broad based interpretation would potentially disrupt a large swath of internet commerce without further refinement as the precise basis of liability, which the court declines to consider."

Unfortunately, the clarity was soon muddled by another Los Angeles Superior Court decision one month later in *Levings v. Choice Hotels International, Inc*. There, the plaintiff only alleged that the defendants "secretly used 'pen register' software to access Plaintiff's device and install tracking software in violation of California law" without any further detail. The *Levings* court held that the allegations were sufficient to state a claim for a CIPA violation and rejected the idea that identifying the precise mechanism acting as a pen register was necessary at the initial pleadings stage. The court did not address the argument that an IP address could not act as that "unique fingerprint" like the *Licea* court did. These split decisions have only emboldened plaintiffs' firms looking for a quick pay day, hoping that companies will opt for an early settlement rather than face drawn out litigation in an uncertain area.

What You Can Do to Avoid Becoming a CIPA Defendant

While the interpretation of CIPA's applicability to the internet and Tracking Technologies reaches higher courts or is addressed in legislation, companies should take action to avoid becoming the next CIPA defendant. Companies should consider defensive measures and other innovative analytics technologies to reduce the attractiveness of their web-based infrastructure to potential claimants. Companies may also want to re-evaluate the potential costs and benefits of continuing to use various Tracking Technologies. Companies should analyze customer engagement workflows in an effort to obtain user consent at the earliest stage of engagement. Finally, companies should ensure their website Terms of Use contain enforceable mandatory arbitration provisions or otherwise dictate a preferred choice of law and venue in the event of a potential lawsuit.

---

[5] *Id*. at § 638.50(c)
[6] *Javier v. Assurance IQ, LLC*, Case No. 20-cv-02860-CRB (9th Cir. May 31, 2022).
[7] *Greenley v. Kochava*, Case No. 22-cv-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023)
[8] *Licea v. Hickory Farms LLC*, Case No. 23STCV26148 (Cal. Sup. Ct. L.A. County Mar. 13, 2024)
[9] *Levings v. Choice Hotels International, Inc.*, Case No. 23STCV28359 (Cal. Sup. Ct. L.A. County Apr. 3, 2024)

This Alert Was Authored By

Kate Campbell | (312) 269-2964 | kcampbell@nge.com

Alfred C. Tam | (312) 269-8461 | atam@nge.com

David Wheeler | (312) 269-5328 | dwheeler@nge.com

Josh Hanson | (312) 269-5982 | jhanson@nge.com

If you need assistance evaluating Tracking Technologies or if you have received a demand letter or lawsuit related to your use of Tracking Technologies, please contact a member of our Cybersecurity & Data Privacy team—Kate Campbell, Alfred Tam, David Wheeler and Josh Hanson—or your Neal Gerber Eisenberg attorney.
