



Privacy & Cybersecurity Update

October 2024

CIPA Pen/Trap Update: From “Absurd Result” Arguments to *Pro Se* Complaints

There has been a substantial increase in legal claims arising from allegations that the use of website tracking cookies and pixels violates the [pen register and trap and trace device \(pen/trap\) provisions](#) within the California Invasion of Privacy Act (CIPA). A July 2024 ruling by the [Central District of California](#) with respect to the use of TikTok marketing pixels has likely served as a catalyst for plaintiffs seeking to identify businesses for potential CIPA violations to serve them with complaints and demand letters. Since this July decision, there has been a flurry of noteworthy judicial rulings in California state courts.

Public Policy and “Absurd Result” Arguments

CIPA is a criminal statute, and an individual who violates its terms can be subject to both monetary penalties and imprisonment. In turn, if a court were to adopt the position that a website advertising cookie or pixel is considered a pen register or trap and trace device, it could subject every organization with a public-facing website that uses this technology (without a court order or other exception) to civil *and* criminal liability. In March 2024, LA County Judge Stephen P. Pfahler took issue with such a broad interpretation and absurd result.

Specifically, Judge Pfahler found that “public policy strongly disputes” such a broad interpretation of CIPA because it would render “every single entity” whose website is “voluntarily visited by a potential plaintiff ... as a [CIPA] violator” and “potentially disrupt a large swath of internet commerce.” (*Licea v. Hickory Farms*, No. 23STCV26148, at 6 (L.A. Super. Ct. Mar. 13, 2024)).

In *Heiting v. Taylor Fresh Foods, Inc.* (No. 24STCV12891 (L.A. Super. Ct. July 31, 2024)), LA County Judge Daniel S. Murphy provided a contrasting opinion on this issue. Here, the judge noted that the plaintiff’s complaint alleged that the TikTok

pixel deployed on the defendant’s website both “tracks data beyond that which is necessary for the proper functioning of a website” and gathers, without the plaintiff’s consent, “unique location information and other information besides IP addresses.” Judge Murphy indicated these allegations are more concerning than those raised in *Licea v. Hickory Farms*. He then quoted the court’s opinion in *Levings v. Choice Hotels Intern.*, stating that “[i]f merely visiting a website constitutes consent to the use of a [trap and trace device], then Section 638.51(a) would be a dead letter. It could never be violated. That is not an acceptable consequence.”

According to Judge Murphy, because the plaintiff alleged that the TikTok pixel on the defendant’s website “collects data beyond that which is necessary for the proper functioning of a website,” the plaintiff is “not attempting to subject every website to liability for simply existing,” and “it would be absurd if simply visiting a website waived any violation of section 638.51, thereby rendering all websites immune from prosecution.”

Failure to State a Claim: Demurrers Granted

California courts continue to struggle with identifying whether the use of common website advertising cookies and pixels should be considered pen registers and trap and trace devices when merely collecting end users’ IP addresses. However, the holdings in *Casillas v. Transitions Optical, Inc.* (No. 23STCV30742 (L.A. Super. Ct. Sept. 9, 2024)) and *Rodriguez v. Plivo Inc.* (No. 23STCV08972) provide a thorough analysis of the issue. In each case, the plaintiff alleged that upon accessing the defendant’s public-facing website, the defendant secretly installed a pen/trap beacon to “collect Plaintiff’s IP address” in violation of CIPA.

Casillas v. Transitions Optical, Inc.

On September 9, 2024, LA County Judge Bruce G. Iwasaki granted Transitions Optical's demurrer with respect to the plaintiff's amended complaint. According to Judge Iwasaki, the plaintiff's CIPA complaint "is one of many nearly identical complaints filed by a self-described tester" and "is noteworthy for pleading a series of hypothetical possibilities," but "few specific facts concerning either Plaintiff or Defendant."

In his ruling, Judge Iwasaki began with a recitation of CIPA's pen/trap clauses, noting the "legislative purpose" behind the law is "to authorize law enforcement to seek orders for telephone surveillance" and it "does not address the privacy rights of Internet users." He then focused on the plaintiff's allegation that the defendant's website unlawfully collected her IP address. According to Judge Iwasaki, however, the collection of an IP address "occurs when any user accesses any website" and "[w]hat makes the internet possible – devices communicating with each other – is the communication of the device's protocol." The judge noted that the plaintiff voluntarily chose to allow the defendant's website to "collect" her IP address because an internet user generates the IP address associated with their device only through making the "affirmative decision" to access a website or an online application. Therefore, according to Judge Iwasaki, CIPA's pen/trap clauses "did not, and does not, criminalize the process by which all websites communicate with all users who choose to access them." Judge Iwasaki used the plain text of CIPA's pen/trap clauses to support his conclusions:

A pen register does not include a "process used by a provider or customer of [an] ... electronic communication service for ... communications service provided by such provider ... or other similar services in the ordinary course of business." (Pen. Code, § 638.50, subd. (b).) Moreover, even if the process of collecting IP addresses is deemed a pen register, there is no liability when an electronic communication service does so to "operate, maintain, and test [an] ... electronic communication service" or to "record the fact that [an] ... electronic communication was initiated or completed" to protect against unlawful or abusive use of the service. (Pen. Code, § 638.51, subd. (b).)

Judge Iwasaki found that the defendant's website is an "electronic communication service" within the meaning of

CIPA and therefore "obtaining IP addresses from ordinary user access does not violate" the law.

In addition, Judge Iwasaki cited *Columbia Pictures Industries v. Bunnell* (C.D. Cal. May 29, 2007, CV 06-1093FMCJCX) and *Capitol Records, Inc. v. Thomas Rasset* (D. Minn. June 11, 2009, No. 06-1497) as "[c]ases interpreting the analogous federal pen register statute" to support his conclusion. He also found that "[e]ven if it is assumed that the ability of a website operator to obtain a user's IP address constitutes operating a pen register," the plaintiff has no reasonable expectation in the privacy of her computer's IP address. This is fatal to the plaintiff's claim because, according to the judge, "[t]o establish her claim that Defendant violated her right of privacy, Plaintiff must establish a specific, legally protected privacy interest in her computer's IP address, and entertain a reasonable expectation of privacy."

Judge Iwasaki also dismissed the plaintiff's reliance on *Greenley v. Kochava* (684 F. Supp.3d 1024 (S.D. Cal. 2023)), which has served as a basis for several of these CIPA pen/trap claims. The defendant in *Greenley* was a third-party data broker, not a website operator, like the case at hand. "Because the conduct of the defendant and the relationship to the plaintiff were quite different from the allegations here, *Greenley* does not support Plaintiff's argument."

Rodriguez v. Plivo Inc.

On October 2, 2024, LA County Judge Mark. E Windham granted Plivo's demurrer with respect to the plaintiff's amended complaint. He began his ruling by citing relevant definitions within CIPA and noting that because there is "no controlling state law cases on this statute" the "Court must look to federal court rulings for guidance." According to Judge Windham, "[i]n determining whether a device is a pen register, courts must look to the type of information being collected and not the device or process" because "what constitutes a pen register has changed as technology has shifted from telephone communication to internet-based communications."

Judge Windham agreed with the defendant's arguments that the plaintiff's IP address is not the type of information CIPA prohibits parties from collecting and that the plaintiff's IP address is not the type of information collected by pen registers.

On the first issue, Judge Windham noted that the plaintiff voluntarily provided her IP address to the defendant when

accessing its website and she could have no expectation of privacy in it. The judge noted that “[t]his is implicit in the allegations explaining ‘the IP address enables a device to communicate with another device – such as a computer’s browser communicating with a server.’”

On the second issue, Judge Windham found that “Plaintiff’s IP address is not the type of information collected by pen registers” and these tools are designed to “collect outgoing information, such as outgoing telephone numbers, outgoing email addresses, IP addresses of websites visited, location data that reveals sensitive information, and cell site information.” He also distinguished the present case from *Greenley*: “Although Plaintiff alleges that the IP address could reveal the device’s state, city, and zip code, this is not the type of sensitive data to which the *Greenley* court referred” and “Plaintiff’s device’s city and zip code information is not analogous” to the sensitive and private data at issue in *Greenley*, such as a person’s religious affiliation, sexual orientation, and medical condition. Like Judge Iwasaki, Judge Windham also cited *Columbia Pictures* to support his conclusion.

New Pro Se Claims

In perhaps one of the more interesting twists in CIPA litigation, there is a *pro se* plaintiff who has filed about 35 complaints in California state court since September 9, 2024. These complaints range from allegations pertaining to violations of California’s Pay Transparency Law to deceptive marketing and false advertising claims to CIPA violations. The CIPA claims focus on the unlawful installation of spyware on defendants’ websites and recording and disclosing communications content without proper consent. The defendants are not limited to any particular business sectors and include media outlets, online dating platforms, and sporting goods stores. Historically, CIPA claims have been initiated by a handful of law firms that often describe themselves as “privacy advocates.” When these law firms reach a settlement with a defendant, they often agree that they do not have knowledge of, or anticipate raising, similar claims against the defendant, which helps minimize risk that the defendant will be sued again by the same law firm in the future. However, the introduction of a *pro se* plaintiff into this process presents the unfortunate situation where companies can be sued by dozens and dozens of plaintiffs who are using “boilerplate” complaints and looking for a quick payout.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Kim Sim Sandell

310.382.1309

Kim.Sandell@ThompsonHine.com

Amanda Schwaben also contributed to this article. Amanda is a Thompson Hine law clerk; she is not admitted to the practice of law.

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.