Published on *The National Law Review* https://natlawreview.com

Criminalizing the Internet – Websites as 'Trap and Trace Devices' Under CIPA

Article By:

Adam D. Bowser

Andrea M. Gumushian

Have you recently visited a plaintiff lawyer's website? If so, then you may be entitled to compensation under the most contrived California Invasion of Privacy Act (CIPA) theory yet.

In a recent surge of CIPA lawsuits and demand letters, the usual suspects have been accusing website operators of "secretly installing tracking software on the devices of all visitors" in alleged violation of California law. Here, as with previous CIPA lawsuits, the plaintiffs claim that the use of online tracking technologies, such as pixels, cookies, and web beacons, are tantamount to the use of a "pen register" (PR) or "trap and trace" device (TTD) that "capture" a visitor's IP address, resulting in the "illegal interception" of communications signaling information under Section 638.51 of CIPA.

CIPA Section 638.51 – Pen Registers and Trap and Trace Devices

Like most statutes within CIPA, the PR/TTD restrictions appear to have been written by a combination of ChatGPT and the "Have You Ever Had a Dream" kid. Specifically, the term "pen register" evolved from a mechanical device used to record telegraph signals on paper to devices used by law enforcement to track numbers dialed from specific telephone lines. Meanwhile, "trap and trace" devices are similarly defined to mean "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." CIPA Section 638.50. These ostensibly broad definitions are then combined with the prohibition in Section 638.51 that no one can use PR/TTDs unless they first obtain a court order or they are the communications service provider using it to operate their service.

So, did California silently criminalize the entire Internet — where every website operator routinely

obtains website visitors' IP addresses — without applying for a search warrant? That's apparently the theory underlying these latest setup claims.

Recent Lawsuits and Allegations

As we've previously detailed, there's been an explosion of cookie-cutter CIPA lawsuits filed by Scott Ferrell and others since the US Court of Appeals for the Ninth Circuit's unpublished *Javier v. Assurance IQ* decision. The plaintiffs' attorneys were further emboldened by the 2023 decision in *Greenley v. Kochava*, which applied CIPA's pen register provisions to the defendant's use of software development kits (SDKs). The court in this case ruled that software capable of identifying consumers, collecting data, and correlating this data through unique "fingerprinting" could be considered a pen register, at least at the motion to dismiss phase, as it allegedly qualified as a process under the statute's definition. Critically, however, the *Greenley* case specifically dealt with the actions of a third-party data broker which allegedly inserted "spyware" code into the SDK of the first-party app developer. In other words, a third-party "eavesdropper" was alleged to have intercepted data and programmed the SDK to automatically reroute app user data to it without consent.

This is a significant distinction because, in typical Ferrell fashion, he takes a marginal case targeting alleged third-party interception and then applies it to *first-party* website operators at the destination. In fact, his latest cookie-cutter Section 538.51 complaint won't even disclose the allegedly offending "beacon by name, the details of its deployment, or the breadth of its operation" in order to "deter 'copycat' litigation." And he alleges this while filing the same copycat complaint over and over again. If only irony was an affirmative defense in California. But luckily, there are still plenty of arguments to beat these meritless claims.

Your Website Is Not a Trap and Trace Device

As noted above, the underlying theories in these cases would effectively criminalize the Internet, as every website collects and stores visitor IP addresses and other signaling information. Indeed, many of the same firms filing these claims use Google Analytics and other "tracking technologies" on their own websites that "capture" and share visitor IP addresses with third parties. This is the CIPA equivalent of "I learned it by watching you!"

Moreover, California has a first-in-the-nation comprehensive privacy law that gives consumers control over their personal data: the California Consumer Privacy Act (CCPA). The CCPA purposely addresses how businesses can *collect* and use consumers' information obtained online, *expressly including their IP address, device identifiers*, etc. It also outlines what disclosures are required and how such disclosures need to be made to consumers. Therefore, the plaintiffs' arguments in these cases are based on the absurd premise that CIPA *silently supersedes* the CCPA and disrupts the careful and comprehensive balance struck between consumer privacy rights and businesses' ability to collect *and* use the *exact information* at issue.

Ultimately, once you dig a little deeper into these trap-and-trace claims, they cannot apply to website operators for numerous reasons. In fact, the *sole purpose* of these sections of CIPA was to *authorize* state and local law enforcement to use pen register and trap and trace devices under state law, and to *permit* the issuance of emergency pen registers and trap and trace devices. In other words, this statute was not enacted to *restrict* any party to a communication, including website operators, from continuing to use information exchanged in the ordinary course of a communication.

Otherwise, anyone using caller ID on their phone without a court order: right to jail, right away.

This is the only reasonable conclusion when analyzing the statutory definition sections, which expressly limit the key terms of “wire communication” and “electronic communication” as applying to the *interceptions* of wire and electronic communications. That is, these definitions expressly do not apply to *stored* communications or stored content. And as we’ve successfully argued in similar CIPA cases, once a consumer reaches the destination website, that is reception, not interception.

Second, and relatedly, the *only* entities capable of using a pen register or trap and trace device under the relevant CIPA sections are “peace officers” pursuant to court orders or “providers of electronic or wire communication service” pursuant to one of the enumerated statutory exemptions, such as with the “consent of the user of that service.” In other words, the only entities encompassed by this statute are *non-parties* to the communication, if any, which further supports the express statutory definitions above that scope is limited to *interceptions*, rather than *receptions* by parties to the communication.

Third, consent is only a defense for the *communication service provider*, not the recipient of the communication, if any. If plaintiffs’ attorneys claim that businesses provide the communication service at issue and were required to obtain consent, then there is a separate statutory exemption for using pen registers or trap and trace devices “to operate [or] maintain … [the] communication service.” Thus, in these scenarios, plaintiffs’ attorneys have no standing to complain about how businesses operate their websites, which is exactly what they are doing.

Fourth, the statutes incorporated by reference into the relevant CIPA sections further state that this statute does not apply to the operation of websites, and in fact, only applies to *telephonic* communications in transit. Specifically, Section 638.52 only contemplates court orders that “*shall* specify … the telephone line to which the pen register or trap and trace device is to be attached.” Another section only authorizes oral approval to install PR/TTDs if the same grounds under Section 638.52 are met. Simply put, communications over the Internet are not even within the scope of the relevant chapter of the California Penal Code. The point being, do not concede that this statute silently applies to Internet data exchanges, when the CCPA was expressly enacted to govern this area.

Ultimately, if you find yourself on the receiving end of a wiretapping demand letter or complaint, know that you have options to fight it.

National Law Review, Volume XIV, Number 158