CIPA Trap and Trace/Pen Register Claims are Technologically and Legally Flawed

*Contributed by **Jason Russell**, **James Pak**, and **Hillary Hamilton**, Skadden*

June 2024

1. Introduction

In 1967, California enacted the California Invasion of Privacy Act (**CIPA**) to prevent illicit wiretapping of landlines to record or eavesdrop on private telephone conversations. Over the years, the legislature made modest amendments and the statute was rarely cited, much less invoked as a basis for claims. However, with the advent of "chat features" on consumer-facing websites, creative plaintiffs' lawyers brought a wave of actions alleging various internet technologies violate CIPA's "wiretapping" provisions. But most of CIPA's provisions were not intended to apply to such technologies. Not surprisingly, courts increasingly rejected claims suggesting prohibitions on telephone wiretapping applied to website chat features. Plaintiffs' firms thus recently pivoted to **CIPA Section 638.51**, which prohibits the use of pen register or trap and trace devices without a court order.

A pen register is "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, but not the contents of a communication." **Cal. Pen. Code § 638.50**. A trap and trace device is "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." In short, a pen register enables the recording of all outgoing numbers from a particular line, while a trap and trace device enables the recording of all incoming numbers to a particular line.

Section 638.51 permits a "provider of electronic or wire communication service" to use a pen register or trap and trace device with consent and/or for certain enumerated purposes, including: to operate or maintain the service, protect the provider's rights or property or users of the service, or record that a communication was initiated or completed to protect a provider or user from fraudulent, unlawful, or abusive behavior. A violation of Section 638.51 is punishable by a fine not exceeding $2,500 or by imprisonment not exceeding one year.

Very few decisions have interpreted Section 638.51 to date. The first court to do so noted that no other court had directly addressed the statute, and characterized certain internet-based software as equivalent to a pen register device in **Greenley v. Kochava**. Plaintiffs' complaints cite this language in the current wave of filings, alleging generally that a website's collection of user-related information constitutes an impermissible use of pen register and trap and trace technology.

Since October 2023, at least 269 actions have been filed in California state and federal courts and the Southern District of New York, alleging Section 638.51 violations. While some of these actions have settled and been voluntarily dismissed, the majority are in the early stages of litigation. Below we describe plaintiffs' theory of liability and certain flaws in that theory that defendants can raise in response to such actions.

2. Plaintiffs Pivot to a New Theory of CIPA Liability

Under CIPA's more general wiretapping provisions, plaintiffs must plead and prove a third party "intercepted" the "contents" of a communication. But many courts have held data most often collected by website operators (e.g., mouse clicks, keystrokes, search terms, scrolling, and pages viewed) does not constitute such "contents." Thus, plaintiffs' firms pivoted to Section 638.51 because it does not require "contents" to be captured, only the interception of metadata—in other words, "dialing, routing, addressing, or signaling information."

Alleged violations under Section 638.51 are premised on the use of technologies such as pixels. These pixels are commonplace on the internet and are used by website operators for different marketing purposes, like gauging user engagement. Numerous technology companies offer pixel-related products, including Meta and Google.

Plaintiffs generally allege that a website owner uses pixels to gather information from a user's device and create a digital profile specific to each user through a process that plaintiffs describe as "digital fingerprinting." Plaintiffs particularly focus on the collection and disclosure of a user's IP address—a string of numbers that can sometimes identify the device a user is using to connect to the internet. Some plaintiffs have also identified other information collected and disclosed using pixels, such as the content that a user accessed or inputted while visiting a given website.

Complaints and demands premised on this theory are relatively easy to put together and require minimal technical analysis of a website. Drafting these allegations requires no specialized knowledge of computers, the internet, or software. Instead, plaintiffs and their counsel can rely on numerous publicly available tools to determine whether pixels are active and, if so, the types of information those pixels are collecting and disclosing.

3. Numerous Defenses Exist to Section 638.51 Claims Based on Internet Communications

Courts have yet to address the numerous flaws in plaintiffs' theory. The most obvious flaw is that it implicates not just pixel technology, but how the entire internet functions. Nearly every internet communication operates using "network packets," the electronic equivalent of packages traveling through physical mail services: the outside label tells the carrier the sender's address, the destination of the package, and its contents. Network packets likewise contain underlying data and a

label which informs computers on the internet where the data is coming from and where it is going. This source and destination information is described using IP addresses that identify devices connected to the internet.

IP addresses are critical to how the internet works. Without them, computers cannot find and communicate with each other: a user would not be able to locate a website, and a website would not be able to send content to a user. It is therefore fundamental that IP addresses be disclosed as communications travel across the internet from computer to computer (including website servers).

But under plaintiffs' theory, *all* communications containing IP addresses directly implicate Section 638.51—any IP address is the internet equivalent of "dialing, routing, addressing, or signaling information," and such information is necessarily collected as network packets travel from one computer to another. This encompasses literally all internet communications, including (ironically) communications between users and the websites of plaintiffs' law firms, for example.

At least one court has already indicated this theory is nonsensical. In **Licea v. Hickory Farms LLC**, the court agreed that "public policy strongly disputes [the] 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," and sustained defendant's demurrer.

Moreover, while plaintiffs may argue the California legislature intended CIPA's trap and trace and pen register provisions to apply to internet communications as "wire" or "electronic" communications, the legislative history indicates otherwise. These provisions were drafted in 2015 in consultation with the Los Angeles District Attorney's Office, Los Angeles County Sheriff's Department, and the ACLU to address concerns about law enforcement use of pen register and trap and trace devices on *telephone* lines without a court order. **2015 California Assembly Bill No. 929, California 2015-2016 Regular Session, Cal. Committee Report, April 6, 2015**. The internet unquestionably existed in 2015, but the new provisions make no mention of internet communications specifically.

If the legislature had wanted to include internet communications, it would have done so explicitly. For example, **CIPA Section 632.01** was enacted in 2016 to prohibit the disclosure of confidential communications with health care providers "in any forum, including . . . Internet Web sites and social media," defined as "an electronic service or account, or electronic content, including, but not limited to . . . instant and text messages, email, online services or accounts, or Internet Web site profiles or locations." **Cal. Pen. Code § 632.01**. The legislature's choice to omit such language from the pen register and trap and trace provisions—even when amending Section 638.50's definitions in 2022—confirms it intended only to ensure law enforcement acted within a person's constitutional right to privacy when it came to monitoring a person's *telephone* communications.

Numerous other hurdles exist. For example, Section 638.51's language regarding court-issued orders expressly addresses actions performed against a *specific individual* that law enforcement is trying to track. In contrast, internet technologies like the pixel operate agnostically, without regard to who the individual being tracked is. And perhaps most importantly of all, Section 638.51 exempts liability where consent is obtained. It is likely that any potential plaintiff would have consented to the use of such internet technologies through the website operator's terms or privacy policy.

It remains to be seen how courts will treat these claims and defenses as the wave of **CIPA** litigation rolls on.

Partners Michael McTigue Jr. and Meredith Slawe and associateRachel Moore also contributed to this article.