2. Website tracking litigation

By Kayla Bushey, CIPP/US

Old state wiretapping laws have inspired vigorous data privacy class-action lawsuits, requiring consumer-facing businesses to determine whether the consumer tracking technologies used on their websites put them at risk of litigation. Among this recent litigation trend is a decades-old wiretapping law from California that has spearheaded privacy class-action lawsuits against businesses using tracking tools on their websites and motivated plaintiffs elsewhere who seek to apply their states' wiretapping laws to digital tracking and analytics.

The CIPA

Since 2022, plaintiffs have filed hundreds of lawsuits alleging violations of the California Invasion of Privacy Act. CIPA is an extensive wiretapping statute passed in 1967 due to rising concerns of eavesdropping amid the advancement of wiretapping technology during the Cold War era. Decades later, plaintiffs allege retail, insurance and manufacturing businesses, among others, use website tracking tools to collect consumers' data in a manner that violates CIPA. Many of these cases focus on Section 631(a), which prohibits intercepting communications while in transit to learn the contents of the communication, although Sections 632(a) and 638 have also been invoked in privacy-related complaints. Section 631(a) has four clauses that can give rise to liability.

The first part of the statute prohibits the intentional tapping of "any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system." Part two prohibits the unauthorized interception and reading of "the contents or meaning of any message, report, or communication while the same is in transit." The third portion of the statute prohibits use of the contents of the communication that was intercepted without authorization. Lastly, the fourth portion prohibits a party to the communication from aiding and abetting any third party attempting to complete any of the prohibited acts listed above.

Section 632(a) requires consent from all parties before recording any confidential communications, while Section 638.51(a) prohibits the use of a pen register without a court order or prior consent from the user.

Parties that violate any of these provisions can face fines of USD2,500 for each violation. Parties that previously violated CIPA can be fined up to USD10,000 for further violations.

What is considered 'contents of a communication' under CIPA?

A CIPA claim follows the same analysis and definitions of the Electronic Communication Privacy Act of 1989, which updated the Federal Wiretap Act of 1968. The ECPA defines contents as "any information concerning the substance, purport, or meaning of (a) communication." However, the statute does not cover record information, such as the metadata of a communication. The contents of the communication must be intercepted while the communication is being made and not at a later point.

Some district courts have allowed CIPA lawsuits to proceed and avoided motions to dismiss in which the complaints sufficiently allege the data points collected — such as the users' clicks, swiping, scrolling, mouse movements, geolocations, IP addresses and typing — were contents within the meaning of the statute. For example, the court in Saleh v. Nike found the plaintiff sufficiently pleaded the defendant's vendor had collected contents communications. Despite information such as "names, addresses, telephone numbers, and email addresses" commonly being record data, this information could become content when entered into a form on the defendant's website.

However, other district courts have repeatedly found plaintiffs failed to allege that the tracking software collected contents at the pleading stage. Some of these decisions hinged on the bare allegations the plaintiffs included in their complaints. Other courts found collecting users' visit dates and time stamps, IP addresses, locations, browser types, device types, and metadata are not content within the meaning of CIPA.

In Yoon v. Lululemon, the court rejected the plaintiff's argument that third-party software intercepted the contents of her communications with the defendant through data about her keystrokes, IP address, location and browser type, among others, because "none of these pieces of data constitutes message content in the same way that the words of a text message or email do."

CIPA litigation leads to circuit splits

In the landmark case in CIPA litigation, Javier v. Assurance Ins., the U.S. Court of Appeals for the Ninth Circuit found Section 631(a) of CIPA covered internet communications and was not limited to traditional phone conversations. The court went further in finding prior consent is required before a consumer's communications with the website can be intercepted by an undisclosed third-party vendor in the form of a recording.

Here, the plaintiff alleged the defendant's use of a session replay software captured the "contents of his communication," which the court defined as his "demographic information and medical history." The court found the plaintiff properly alleged the third-party software company captured his actions in real time without his prior consent and allowed the claim to survive the defendant's motion to dismiss.

However, the Ninth Circuit is split on how to interpret other parts of Section 631(a).

Is the tracking software an extension of the defendant or an illegal third-party eavesdropper?

A circuit split emerged regarding whether a vendor that provides tracking technology is a third-party eavesdropper within the scope of CIPA. Section 631(a) holds third-party eavesdroppers and parties that aid and abet these eavesdroppers liable for intercepting a party's communications. Therefore, plaintiffs must allege the third-party tracking tools are illegal third parties under the statute.

Courts have differed on whether a third party's software acts as an extension of the defendant, as a tape recorder by only storing the consumer's data, or if it acts as a traditional eavesdropper. Courts have found tracking software that acts as a mere tape recorder does not intercept the consumer's communications with the defendant's website and, therefore, does not give rise to liability under CIPA.

For example, in Graham v. Noom, the court found the defendant's vendor, a session replay software company, did not use the data for its own benefit but instead collected information solely for the defendant's benefit. Thus, the court reasoned the software vendor's use of the data was comparable to that of a tape recorder. Since the vendor did not make further use of the visitors' data, its conduct did not give rise to liability under the statute.

To survive a motion to dismiss at the early stages of litigation, plaintiffs must allege the tracking software acts as a traditional eavesdropper and has the capacity to utilize the collected data for uses other than reporting analytics to the defendant. Indeed, courts have found software that instead acts as an eavesdropper to the communications between the consumer and the defendant will give rise to liability under CIPA if the consumer has not provided prior consent.

In the Javier case, for example, the court found a defendant's vendor could be a third-party eavesdropper if it had the capacity to use the collected data for its own benefit and further uses. In another example, the court in Rodriguez v. Ford Motor Co. found the plaintiff sufficiently alleged the defendant's software as a service provider had the capacity to do more than store the website's chat communications and could use it to create an extensive customer dataset to use for its own purposes.

Are tracking technologies unlawful pen registers under CIPA?

More recently, courts have been split in determining whether website tracking technology fits within the definition of a pen register under CIPA, and courts have allowed plaintiffs past the pleading stage.

In Greenley v. Kochava, the leading decision for CIPA pen register claims, the court found the plaintiff sufficiently alleged the defendant's embedded tracking software was a "process" under CIPA's definition of a pen register.

However, in Licea v. Hickory Farms, the district court rejected the plaintiff's argument that the defendant used a pen register to collect IP addresses from its website. The court granted the defendant's motion to dismiss because the plaintiff failed to allege what device or process operated by the defendant constituted a pen register. Further, the court distinguished this

complaint against allegations in Greenley by stating the collection of IP addresses vastly differed from the unique digital fingerprint alleged by the plaintiff in the prior case. The court also emphasized public policy rejects the plaintiff's interpretation of CIPA because every entity that collects an IP address from a potential plaintiff would be in violation, an interpretation that "would potentially disrupt a large swath of internet comm erce."

Yet, a month later in Daryl Levings v. Choice Hotels International, the same district court found the plaintiff sufficiently alleged the use of a pen register when the defendant used software to collect information transmitted from the plaintiff's device and install a tracking code. The court rejected the defendant's motion to dismiss by concluding the plaintiff met their burden at the pleading stage and "a detailed description of the software and precise mechanism it employs are evidentiary facts which need not be included."

In Gabrielli v. Insider, the court dismissed a CIPA pen register claim in February 2025 after finding the plaintiff lacked standing. The plaintiff alleged the defendant's use of a third-party tracker on its website, which logged visitors' IP addresses, constituted an illegal pen register.

Article III of the U.S. Constitution provides federal courts the power to hear only cases or controversies. To satisfy this requirement, plaintiffs must allege they have standing to bring a claim in federal court by showing they suffered from an injury-in-fact, meaning an injury that is concrete, specific and can be traced to the defendant's conduct. Under current U.S. Supreme Court jurisprudence, if a plaintiff bringing a privacy-related claim cannot show a concrete harm, in which the injury has a close relationship to a traditionally recognized harm, they do not have standing to bring a claim.

In a motion to dismiss, the defendant argued the plaintiff lacked standing because they failed to show how sharing IP addresses with third parties was a concrete harm. The plaintiff argued the disclosure of visitors' IP addresses to third parties for the defendant's profit is an invasion of privacy recognized at common law. The court rebuffed the plaintiff's arguments, concluding an IP address does not reveal personal information of a visitor but instead only provides general geographic information as specific as a zip code. The court concluded the general information provided by an IP address does not constitute an invasion of privacy and therefore is not a concrete harm. In doing so, the court dismissed the plaintiff's claim for lack of standing with prejudice, barring the plaintiff from amending or refiling this claim.

Although the judges in Gabrielli and Hickory Farms both dismissed plaintiffs' pen register claims that alleged tracking technologies merely collected IP addresses, the Gabrielli decision may have a further-reaching impact as courts may now dismiss CIPA pen register claims at the outset of a lawsuit with similar arguments. However, Gabrielli does not preclude future CIPA pen register cases in which plaintiffs can sufficiently allege detailed personally identifiable information

was disclosed to a third party using tracking technology like the plaintiff in Greenley.

Ultimately, the new wave of CIPA pen register claims may have been hindered, but businesses should still be aware of the remaining strength of this claim.

Rise in CIPA lawsuits for consumer tracking technologies

Plaintiffs' lawsuits focus on the technical aspects of various tracking tools and how these tools allegedly provide third parties with confidential communications without the users' consent, in violation of CIPA. These tools include session replay software, chatbots and pixel trackers, among others.

Session replay software

Session replay software provides website operators with visual playbacks or video recordings of users' actions on websites. It is commonly used by businesses to seamlessly view how users interact with their webpages and to troubleshoot issues consumers may have while using the webpages.

Case study: Javier v. Assurance

In Javier, the plaintiff used the defendant's website, where he input the required personal information to receive an insurance quote. The defendant had installed session replay software from a vendor on its website, allowing it to record a visitor's entire interaction with the webpage.

Chatbots

Chatbot and chat software provide consumers with real-time virtual assistance in the form of written communications while browsing a business's webpage. However, chatbots are often created and operated by third-party vendors, leading to lawsuits for conversations that are transmitted to the third party in real time for the chatbot to answer the user's question or prompt.

Case study: Jones v. Peloton

The plaintiff in Jones v. Peloton challenged the defendant's chat feature on its website because it embedded third-party software into the chat function to intercept and transmit visitors' communications to the third-party. Here, the court found the plaintiff failed to allege that the third-party was an eavesdropper and therefore granted the defendant's motion to dismiss.

Pixel tracking

Pixel tracking provides website operators with the ability to track user events and actions throughout visits to websites. Pixel tracking is a unique piece of code that allows the business to customize what user actions, such as clicking a button or image on the webpage, it would like to track. Many pixel tracking codes are free and provide businesses the option to install the code manually or with a partnered software vendor.

Pixel tracking allows the business to see how many user actions occur and how users interact with the website to improve their advertising. The pixel also sends user actions to the company that originally wrote the pixel code and can allow it to customize the users' ad placements while using its platforms.

Case study: Griffith v. TikTok

In Griffith v. TikTok, the plaintiff brought a claim under Section 631(a) and Section 632 against TikTok for the pixel code it provided to various online websites. In the complaint, the plaintiff maintained she had never created a TikTok account or utilized the platform due to privacy concerns, but TikTok obtained her personal information through its pixel code installed by websites like Hulu and Etsy. The court rejected the defendant's motion to dismiss because it failed to show the information collected by the pixel was not confidential, to prove the code was not used as a tape recorder and to provide any legal authority on why it should not be a liable third party for its tool.

Email marketing tools

Email tracking tools allow consumer-facing businesses to track when a potential or returning customer clicks a link in an email advertisement sent by the business. By using a third-party software, the email's words and images contain unique and traceable links to the consumers' email addresses and their actions. These actions are transmitted to the third-party software vendor and then later to the consumer-facing business. This can provide the business and the third party with information about consumer actions, like placing items in a virtual shopping cart. This allows the business to email consumers to encourage them to finish completing their purchases or notify them when products in their carts reduce in price.

Case study: Ramos v. The Gap

At issue in Ramos v. The Gap was the defendant's use of an email tracking software that embeds code on the defendant's emails to past and potential customers. Here, the court rejected the plaintiff's argument that the tracking software could reveal any further information other than the record information for the email, ultimately dismissing the plaintiff's complaint.

Pen registers

Pen registers and trap-and-trace devices are traditionally physical devices that are attached to a telephone line to log all the telephone numbers of incoming and outgoing calls. Plaintiffs alleging violations of CIPA's prohibition on pen registers argue the tracking technology collects information like IP addresses, browser types and locations to create user profiles or fingerprints, which are later shared with the third-party vendor and fit within CIPA's definition of a pen register. Plaintiffs argue the digital profile that is collected and shared is akin to sharing the incoming and outcoming telephone numbers that a traditional pen register or trap-and-trace device would perform.

It is important to note the provision regulating pen registers is applicable to both contents of a communication and record information.

Case study: Greenley v. Kochava

As discussed above, the plaintiff in Greenley v. Kochava alleged the defendant, a data broker, installed unlawful pen registers in the form of its software development kits in violation of CIPA Section 638.51. Plaintiffs argued software developer clients of the defendant used the SDKs to develop their own apps and in exchange allowed the defendant to "surreptitiously intercept location data" from users of the apps and created a unique fingerprint from each device. The plaintiffs then alleged the defendant sold the surreptitiously intercepted data to other clients in consumer-facing industries.

The court in Greenley rejected the defendant's motion to dismiss, finding the plaintiff sufficiently alleged the defendant's SDK could be a pen register under the expansive language of Section 638.51 of the statute. The court reasoned, since the plaintiff had properly alleged the SDK kits collected users' location data, it fit the definition of a pen register. Further, since the SDK kits were installed without a court warrant, the pen register was unlawful and the claim could survive a motion to dismiss.

Notable settlements

In Katz-Lacabe et al v. Oracle America, the defendant software company settled a class-action lawsuit for USD115 million after a federal district court rejected its motion to dismiss the plaintiffs' CIPA allegations. The plaintiffs argued the defendant's proprietary JavaScript code, which was hosted on various third-party websites, surreptitiously collected their personal information to create a "digital dossier" or digital fingerprint, which it later sold to third parties, in violation of CIPA. The court found the plaintiffs sufficiently pleaded enough facts to allege a CIPA violation and avoid the defendant's motion to dismiss.

In July 2024, Oracle announced it reached a settlement agreement with the plaintiffs in which the company would pay USD115 million and agreed to implement specific privacy measures to its existing products, while denying any wrongdoing. The settlement was approved in November 2024; however, it has since been appealed. The software company ended its advertising business in September 2024, citing a fall in revenue.

How can entities comply with CIPA while using analytic tracking technologies?

Businesses can take various steps to mitigate the risk of potential CIPA violations. Privacy notices and terms of use policies should be readily available to website visitors and should detail the types of trackers used on the business's website. The notice should also inform visitors of what data will be collected while using the website, along with a mechanism for users to opt out of the data collection.

Because the Ninth Circuit is split on what information may be "contents of a communication" under CIPA, businesses must clearly inform website users what information will be collected by the tracking tool while using the site. By providing an option for users to opt out of data collection, they can consent to the use of these tracking tools and their data collection.

Further, businesses should consider utilizing cookie banners to disclose the tracking software used on the website, note what data will be collected and provide an option for users to affirmatively consent to the data collection. Along with providing sufficient information in both cookie banners and privacy notices, these must be conspicuous and clear, and conform with state and federal laws.

Businesses should also consider configuring the settings of tracking software to limit or reduce the amount of personally identifiable information to collect only the data needed to provide necessary analytics. They should also consider discontinuing and deleting trackers that are unnecessary or redundant to avoid over-collecting data that could be interpreted as content under CIPA and other wiretapping laws. Although much of the information collected by these trackers may look like record data on its face, the court in Saleh v. Nike found the manner of collection can transform record data to contents and create liability under Section 631(a).

Another consideration for businesses using third-party tracking software is understanding what the third party intends to do with the collected information. As discussed in Graham v. Noom, third parties that do not use the collected data for their own benefit will not create CIPA liability for businesses. Nonetheless, businesses should closely review procurement contracts and monitor third-party vendors to ensure their conduct will not leave them at risk for litigation.

As litigation under CIPA continues, businesses using tracking technologies must closely monitor ongoing decisions and make sure their tracking tools are reasonable, proportional and well maintained to limit the collection of personal information that can lead to unnecessary and expensive litigation.