Tide May Be Turning in Businesses' Favor After Key California Court Decisions in Website Tracking Cases

Insights
2.10.25

Two recent court decisions have provided businesses with long-awaited clarity on the reach of the California Invasion of Privacy Act (CIPA) – and could begin to redefine digital privacy litigation for the better. Two separate California state courts dismissed claims involving website tracking technologies last week, providing solid defenses for businesses to deploy if faced with similar threats or lawsuits. For the last three years, businesses operating websites accessible in California have been facing an onslaught of litigation claiming CIPA violations based on a website's use of third-party cookies, pixels, and other tracking technology. While some courts have given plaintiffs some leeway to proceed on these novel theories, these two decisions might signal that the tide may be turning. This Insight will review these recent decisions and discuss whether they could set crucial precedent for companies navigating compliance with state privacy laws.

Digital Wiretapping Litigation Trend

The trend of digital wiretapping litigation began in California but has since spread across the U.S. Based on public filings we are tracking in our Digital Wiretapping Litigation Map, 1,641 of these lawsuits have been filed in 28 states since June 2022. Of those public filings, 1,361 were filed in California alone – 83% of all claims. As many of these claims are being filed in private arbitration and others are being resolved without any publicly filed lawsuits, we estimate that the number of businesses affected is closer to 5,000.

As Fisher Phillips described in an Insight earlier last year, the claims involve the use of all types of digital tracking technologies such as cookies, pixels, and beacons embedded in websites, apps, or marketing emails. The premise for many of these claims is that a website engages in wiretapping if it is configured to automatically activate third-party cookies the second (or nanosecond) that a user navigates to the website and if that results in disclosure of the user's IP address and other data that can be used by the third party to potentially identify them through their unique browser or device identifiers. According to the plaintiffs in these lawsuits, informing website visitors about this disclosure in a privacy policy or cookie banner and providing them the opportunity to opt out does not remedy the alleged failure to obtain opt-in consent prior to the sharing of data through cookies.

New Theory: "Trap and Trace" or "Pen Register"

One of the theories being asserted in California is that a web beacon encoded into a website violates the CIPA's prohibition on use of a "Trap and Trace device" or "pen register." A "trap and trace device" is a device that captures the incoming signaling information reasonably likely to identify the source of an electronic communication. A "pen register" is 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.

While three federal district courts have denied motions to dismiss claims alleging this theory, these decisions rely upon an interpretation of California law that has so far been rejected by the majority of state courts judges to have ruled on this issue. Below we discuss the most recent of these state court rulings rejecting the "trap and trace device or pen register" theory under CIPA.

Groundbreaking Ruling: *Cars.com* Decision Limits CIPA's Scope

In *Sanchez v. Cars.com Inc.* (February 4), the plaintiff was a self-described "tester" – which means she was not the intended user of the website in question, but rather someone whose job appears to be to trawl websites looking to entrap businesses with these claims. These testers know exactly what to look for and, in their allegations, pretend like they did not consent to the website's data collection and sharing practices, or act is if they have been living under a rock and don't understand how the internet works. It's also not uncommon for the real "testers" to be the law firms filing these lawsuits along with their technical consultants, and they just recruit clients looking for easy money to serve as plaintiffs (it is common to see the same tester plaintiff names in lawsuits filed by the same law firms).

This "tester" plaintiff in this case alleged that Cars.com deployed a tracking beacon on her device that recorded and transmitted her IP address to a third-party service provider when she visited the website. She claimed that the defendant violated CIPA by installing the beacon without her knowledge or consent.

The California Superior Court, however, firmly rejected this expansive interpretation, stating that CIPA was designed to address telephone wiretapping – not routine website tracking. In what may prove to be a pivotal turning point for online privacy litigation, the court ruled that website tracking technologies – specifically, software that logs a user's IP address – do not fall under CIPA's "trap and trace" and "pen register" restrictions. This marks one of the first definitive judicial interpretations to find that CIPA's scope was never intended to regulate standard website analytics.

Additionally, the court underscored that website users do not have a reasonable expectation of privacy in their IP addresses when they voluntarily interact with websites. IP address data is inherently generated when users access a website or online application. By choosing to visit the defendant's website, the plaintiff effectively consented to the collection of this information. As a result, the plaintiff had no legally recognized expectation of privacy in her IP address.

Significantly, the court dismissed this CIPA "trap and trace" claim without leave to amend, which means the case is over as the court concluded that there are no possible facts the plaintiff could add to the complaint that would establish any theory of liability based on disclosure of an IP address through digital tracking technology on the website.

The *LiveRamp* Case Highlights Need for Precision in Privacy Allegations

Another significant ruling came down the exact same day, as the court in *Aviles v. LiveRamp, Inc.* (February 4) reinforced the need for specificity in privacy litigation. Similar to *Cars.com*, the plaintiff alleged that LiveRamp deployed a tracking beacon to collect IP addresses and device information. However, the court found the allegations too vague to move forward. While allowing the plaintiff an opportunity to amend the complaint, the court made clear that privacy claims must precisely articulate how a company's data collection practices differ from how the internet normally works.

The *LiveRamp* court also provided a critical explanation of why website beacons do not qualify as pen registers or trap and trace devices under CIPA. Traditionally, pen registers record the outgoing numbers dialed from a telephone. The beacon in question merely recorded the IP addresses of computers visiting the website. In other words, for the beacon to be classified as a pen register on a computer, it would need to track outgoing IP addresses – such as those of websites visited by the computer – rather than merely capturing the computer's own IP address. Likewise, the beacon could not be considered a trap and trace device because it recorded visitor IP addresses from those accessing LiveRamp's website, making it akin to a tracking mechanism on LiveRamp's system rather than on an individual user's device.

Other Favorable Decisions in CIPA Litigation

Cars.com and *LiveRamp* join a growing pool of case law that rejects broad applications of CIPA to website tracking technologies. Several courts have followed suit, further reinforcing limitations on CIPA claims:

- *Rebeka Rodriguez v. Plivo Inc.* (Cal. Sup. 24STCV08792, Oct. 2, 2024): A website user cannot pursue a CIPA claim based on IP address collection alone, as IP addresses do not constitute outgoing communications data nor contain inherently private information, such as religious beliefs, sexual orientation, or medical history.
- *Marielita Palacios v. Fandom, Inc.* (Cal. Sup. 24STCV11264, Sept. 24, 2024): Software that collects the IP address of website visitors is not a pen register because it does not collect outgoing information.
- *Rebeka Rodriguez v. Fountain9, Inc.* (Cal. Sup. 24STCV04504, July 9, 2024): A website user cannot sustain a CIPA claim without demonstrating a concrete injury resulting from a beacon's collection of their IP address.
- *Miltita Casillas v. Transitions Optical, Inc.* (Cal. Sup. 23STCV30742, Apr. 23, 2024): A CIPA claim is [illegible] if the plaintiff fails to specify how their interactions with the website [illegible]

inadequately pleaded if the plaintiff fails to specify how they interacted with the website, what specific data was recorded, or what software allegedly violated CIPA.

- *Jose Licea v. Hickory Farms LLC* (Cal. Sup. 23STCV26148, Mar. 13, 2024): A website user's CIPA claim is inadequate without specifying what device was used when accessing the website or how their information was acquired. Additionally, penalizing a business for individuals who voluntarily visit and provide an IP address to connect to the business's website contravenes public policy.

Not-So-Favorable Decisions: The CIPA Landscape Remains Unsettled

Despite this recent direction towards favoring businesses, past contrary conclusions indicate that CIPA litigation remains unsettled. In addition to several decisions from federal trial courts interpreting California law and denying motions to dismiss by defendants, several state courts have also refused to dismiss these claims. For example, one state court found that a CIPA claim can proceed as alleged by the plaintiff because software capturing incoming user information can be a trap and trace device under CIPA and a business installing such software on its website may be liable. Another state court found that a CIPA claim can proceed if it describes a website's tracking software as identifying its users, collecting data, and matching that data with existing data.

The plaintiffs' firms filing these CIPA claims may have been emboldened by a few decisions where courts refused to dismiss the claims. However, at the initial pleading stage of any case, a court's refusal to dismiss the claim does not mean that the claim actually has any substantive merit. The bar is very low for claims to survive dismissal, as the court must assume for purposes of deciding the motion to dismiss that the factual allegations in the complaint are true even if they are completely made up. The question before the court is strictly whether there could be liability if the alleged facts are proven to be true. Thus, a court's refusal to dismiss CIPA claims does not necessarily mean it's game over for the internet as we know it.

Moreover, none of these trial court decisions are binding precedent, especially those by federal courts as federal courts are not the final arbiter of California law. To date, there has not been any decision from a California appellate court on the viability of these types of CIPA claims. Until such a binding decision is issued, the hope for businesses facing these lawsuits is for the court to follow the sound reasoning of the growing number of state court decisions rejecting these claims.

Key Takeaways

The *Cars.com* and *LiveRamp* decisions could have a far-reaching impact on the future of privacy litigation in California and beyond. These rulings suggest that courts are unwilling to stretch wiretapping statutes beyond their original intent, signaling a potential shift away from the recent wave of aggressive CIPA lawsuits targeting businesses for standard online tracking practices.

To stay ahead of legal challenges, businesses should:

- **Ensure transparency in privacy policies** to prevent misinterpretations of data collection

practices.

- **Conduct periodic reviews of tracking technologies** to confirm compliance with evolving legal standards.
- **Stay informed on regulatory changes** and emerging case law that may impact digital data collection.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the author of this Insight, or any member of our Privacy and Cyber team.

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Rachel Song
Associate
415.926.7651
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Litigation and Trials

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Digital Wiretapping Litigation Map