Judge Tosses California Digital Wiretapping Claim: Here's the Good News + Lessons for Businesses

Insights
10.22.25

A federal judge in San Francisco just gave website operators a major win, calling the California Invasion of Privacy Act "a total mess" – but the ruling also highlights major privacy risks businesses still face nationwide. Plaintiffs' lawyers across the country have been using old wiretapping laws like CIPA to bring novel claims against website operators that use a third party to perform data analytics and targeted advertising. Friday's decision offers welcome relief to businesses while underscoring the complex and ongoing compliance challenges any business with a website continues to face. Here's what you need to know about the ruling and key steps you should consider taking now.

What's at Play?

CIPA was originally enacted in 1967 to combat traditional wiretapping and eavesdropping, primarily in the context of telephone communications. It was written prior to the internet and was never designed to address the complexities of the digital age or to regulate how businesses track user interactions on the internet.

In recent years, however, plaintiffs' attorneys have increasingly applied CIPA to modern online contexts. Using FP's Digital Wiretapping Litigation Map, we've tracked lawsuits using the statute to target routine website technologies such as cookies, pixels, search bar/form, chatbots, session replay tools, and software development kits (SDKs).

These website technologies are widely used to provide analytics and stats on website traffic, improve website functionality, enhance customer experience, and target ads to website users. Plaintiffs' attorneys, however, argue that these technologies amount to illegal "wiretapping" under CIPA, even though they are standard practices across virtually all commercial websites. This claim is premised on two key assumptions, which some courts have accepted at the pleading stage, that a user's interaction with a website is a communication under the wiretapping law and that metadata collected through cookies about a user's activity on a website is "content of a communication."

The impact is huge: potentially any business with a website or app can fall victim to a digital wiretapping lawsuit.

What Happened in This Case?

- The plaintiff is a California resident who visited a company's website to learn about certain health treatment options. She claims she took a self-assessment, and the data conveyed a strong possibility that she had a particular health disorder.
- According to the complaint, the website operator said it would not collect visitors' personal information or share or sell their personal information to a third party. But the plaintiff began receiving ads on social media from the company and other health services.
- The plaintiff sued under CIPA, claiming the website operator improperly used a third party to perform data analytics and targeted advertising.
- According to the court, "liability here turns on whether the third party 'read' or 'attempt[ed] to read' or attempted 'to learn' the contents of an internet communication between the plaintiff and the website operator while that communication was 'in transit'." If so, the website operator could be liable under CIPA for allowing the third party to engage in such conduct.
- The tracking technology in this case captured event data such as the specific URL of each page browsed by the visitor, the amount of time the visitor spent on the page, the path the visitor took to get to that page, and certain activities like button clicks and inputted answers.
- The third party testified that before logging the data it obtains from websites, it filters URLs to remove information it doesn't want to store, including information that it views as privacy protected.

What Did the Court Decide?

The court sided with the website operator, noting that "using a third-party company to perform data analytics for web traffic is worlds different from wiretapping and eavesdropping."

The court further reasoned that the evidence is undisputed that the third party "did not read, attempt to read, or attempt to learn the contents of" the plaintiff's communications with the website operator while those communications were in transit. It granted summary judgment to the website operator on the CIPA claim.

In reaching his decision, Judge Vince Chhabria of the US District Court for the Northern District of California made his view of CIPA and digital wiretapping claims clear.

> *"The language of CIPA is a total mess. It was a mess from the get-go, but the mess gets bigger and bigger as the world continues to change and as courts are called upon to apply CIPA's already-obtuse language to new technologies."*

He noted that courts are issuing conflicting rulings, and companies have no way of telling whether their online business activities will subject them to liability.

Does the State Legislature Need to Step In?

Judge Chhabria called on the California Legislature to take action. "It would be bad enough if CIPA were merely a civil statute that allowed plaintiffs to recover actual damages for violations. But CIPA imposes criminal liability and punitive civil penalties. Under these circumstances, it is imperative for the Legislature to bring CIPA into the modern age and to speak clearly about how the kinds of activities at issue in this case should be treated." Until then, he said, "courts should generally resolve CIPA's many ambiguities in favor of the narrower interpretation."

Unfortunately, efforts stalled out in the 2025 California legislative session, leaving businesses vulnerable at least until next year when SB 690 may be taken up again. SB 690, as currently written, would:

- Exempt activities conducted for commercial business purposes from several core CIPA provisions
- Shield businesses from liability for the interception or recording of communications when done for a commercial business purpose
- Clarify that the use of pen registers and trap and trace devices for commercial purposes is not a CIPA violation
- Eliminate the private right of action for many online tracking claims conducted for commercial business purposes

California state and federal courts remain divided on the viability of these claims under CIPA. Some federal courts have dismissed these claims for lack of standing to bring the lawsuit because disclosure of IP addresses and device identifiers could not possibly cause concrete harm of the type recognized in common law invasion of privacy torts.

Other judges, sometimes in the same courthouse, have refused to dismiss such claims. In one recent win for website operators, a court found that a website tracker was not a "trap and trace" device under CIPA. Still, courts are reaching diametrically opposed decisions on standing, jurisdiction over non-California businesses, and the merits of the CIPA claims. If the Legislature does not act next year to address this issue, businesses will continue to face these shakedown lawsuits for years to come.

What Should Businesses Do Now?

You should consider taking proactive steps to protect your business and limit your CIPA exposure while we await any future legal developments:

- **Do Not Rely on CCPA Compliance:** Compliance with consumer privacy laws like the California Consumer Privacy Act (CCPA) will not immunize you from risk of CIPA litigation. The claims being asserted under CIPA have nothing to do with CCPA compliance. Although the CCPA does not require you to obtain opt-in consent from website users before cookies fire up and share

data with third parties, plaintiffs in CIPA litigation are claiming that failure to obtain opt-in consent results in wiretapping.

- **Review Website Tracking Tools:** Carefully audit all website tracking technologies in use, including cookies, pixels, chatbots, and similar tools. Ensure these technologies are necessary for your operations and that their use is thoughtfully limited to what is appropriate.
- **Ensure Transparent Consumer Disclosures:** Make sure privacy policies and website disclosures clearly and accurately explain how consumer data is collected, used, and shared. Disclosures should specifically address the use of web tracking technologies and provide users with accessible information about their rights under relevant state consumer privacy laws.
- **Assess and Strengthen Consent Practices:** Whether and how to obtain consumer consent is a risk tolerance issue that each business must address. If your business wants to avoid risk, evaluate whether consumer consent is properly obtained, especially for tracking tools that may trigger heightened scrutiny under CIPA. Consent mechanisms should be clearly presented, easy to understand, and aligned with best practices for affirmative consent where appropriate.
- **Seek Legal Guidance:** It is critical for businesses to actively partner with legal counsel to manage risk and stay ahead of emerging trends.

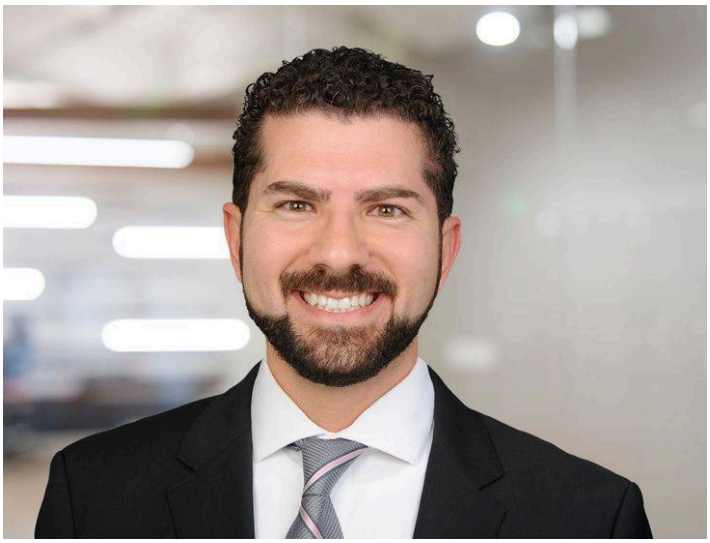
Conclusion

To stay informed, subscribe to Fisher Phillips' Insights System for timely updates on CIPA and other privacy-related trends. For personalized guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Digital Wiretapping Litigation Team. You can also explore additional resources on our U.S. Privacy Hub at any time.

Related People

Catherine M. Contino
Associate
610.230.6109
Email

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Digital Wiretapping Litigation

Trending

U.S. Privacy Hub