California Court Rejects Attempt to Expand Third-Party Eavesdropping Claims to Internet Communications: How Your Business Can Mitigate Risk

Insights
4.22.25

Businesses just received some good news when a federal court dismissed a California Invasion of Privacy Act (CIPA) claim that aimed to expand the reach of the state's wiretapping law to cover internet communications. The April 18 order is the very first ruling to decide, on the merits, whether CIPA could support litigation over the issue of third-party website cookies since CIPA litigation exploded over the last three years. Last week's decision that granted summary judgment to the defendants keyed in on the fact that the third party's accessing of internet communications did not occur while the data was "in transit," but instead involved communications that had already taken place. The big questions we're all asking now: How will this decision impact current CIPA litigation? Will we start to see the tide turn in businesses' favor? And what can this decision teach you about risk mitigation of third-party technology you likely use on your website?

What Happened?

In *Torres v. Prudential Financial, Inc.*, the court just granted a Motion for Summary Judgment filed by Defendants (ActiveProspect, Prudential Financial, and Assurance IQ), which sought dismissal of plaintiffs' CIPA claim.

- The individuals who brought suit allege the website operator (Prudential) and its third-party marketing software platform (ActiveProspect) violated the wiretapping provision of CIPA.
- This broad statute creates liability for anyone who reads, attempts to read, or otherwise learns the contents of any communication made over any "wire, line, or cable" without full consent from all parties. A groundbreaking 2022 federal appeals court decision extended the reach of this statute to website usage.
- Prudential's website enabled users to obtain a quote for life insurance. The company used ActiveProspect's TrustedForm script as part of the website's source code, which plaintiffs alleged enabled ActiveProspect to intercept and record visitors' real-time interaction with the form.
- ActiveProspect allegedly used the data it collected to create a "session replay," which is a recreated video recording of the user's real-time interaction with the form. Plaintiffs alleged that they did not consent to the recording of their interaction with a third party when they completed

the form, which required visitors to enter information regarding their demographics, family, situation, and medical history.

- In November 2024, a California federal court granted class certification to the claim in what appeared to be a first-of-its-kind decision. You can read more about the class certification here.

What is a Motion for Summary Judgment?

A motion for summary judgment is a request to the court to decide the case without a full trial. A party argues that there are no genuine disputes of fact in the case, and the law supports their side. This is typically filed after development of the record through discovery, including depositions.

Last Week's Decision is a Solid Win for Businesses

CIPA creates liability where a person willfully and without consent of all parties reads or attempts to read the contents of the communication while in transit. A participant to a conversation who uses a tape recorder to record a communication, even secretly, is not liable under CIPA.

- The court rejected defendants' first argument that ActiveProspect was a "participant" to the conversation. The court found that this software was not a party to a consumer's communications on Prudential's website through its online form. It cited evidence in the record that demonstrated employees of the software company could view session replays (despite evidence that such access was for customer support purposes). Therefore, the software did not function as a mere "tape recorder."
- However, the court found that ActiveProspect did not read or attempt to read the contents of individuals' communications with the Prudential website while in transit. The court found that even if the third-party software intercepted the contents of individuals communications with the website, there was no evidence that the third party reads or tries to read the contents of the communication ***while it is in transit***. Although the court acknowledged that CIPA was meant to be interpreted broadly to include new technology, the plaintiffs' requested interpretation went too far.
- Allowing this claim to proceed without any evidence that the communications were read in transit, or because ActiveProspect "could have" learned of the contents "would stretch CIPA's statutory language too far to interpret 'while … in transit' to encompass any hypothetical future attempt to read or understand the meaning of a communication."
- Without any evidence that ActiveProspect "independently attempted to decipher the contents of any communication," the court rejected plaintiffs' CIPA claim.

Impact of Decision

This decision demonstrates the court's restraint in broadly applying CIPA's wiretapping prohibition to internet communications. The court outlines what a plaintiff needs to prove to be successful on

these claims, which can assist businesses in mitigating potential risk when utilizing this type of technology.

While the plaintiffs in this case still have one cause of action left (Invasion of Privacy under the California Constitution), their potential damages are much more limited. By granting summary judgment on the CIPA claim, the court ensured that the plaintiffs will lose out on the chance to recover statutory damages of $5,000 per violation – which represented the most valuable part of their claims.

What Can Your Business Do To Mitigate Risk?

With legal theories under CIPA continuing to expand, businesses operating websites must closely examine online data collection and sharing practices. To mitigate the growing risks, you should consider taking the following steps:

Understand How Third Parties are Using Your Data: If you use third-party software on your website, understand how those entities are collecting, storing, and sharing data, allowing for proactive compliance strategies. Conduct regular data mapping exercises to understand exactly how data is captured, used, and stored. Take steps to ensure that the third parties do not attempt to read or access the contents of transmissions of data between the user and your website while the user is interacting with the website. Accessing the contents of such transmissions after the end of the user session may present other legal risks to consider, but at least you would be able to document how third parties do not view the data while the communication is in transit.

Consider Your Consumer-Facing Policies: Review and revise consumer facing policies to include clear provisions on data collection, user consent, and dispute resolution.

- **Notice and Disclosure**: Review and revise online privacy policies and terms of use to explicitly inform users about the collection and sharing of search term data collected through website search boxes.
- **Class Action Waivers**: Help mitigate potential legal exposure and control litigation risk by incorporating class action waivers into terms of use.
- **Dispute Resolution**: Include specific dispute resolution procedures, such as mandatory arbitration, to further protect against litigation risks.

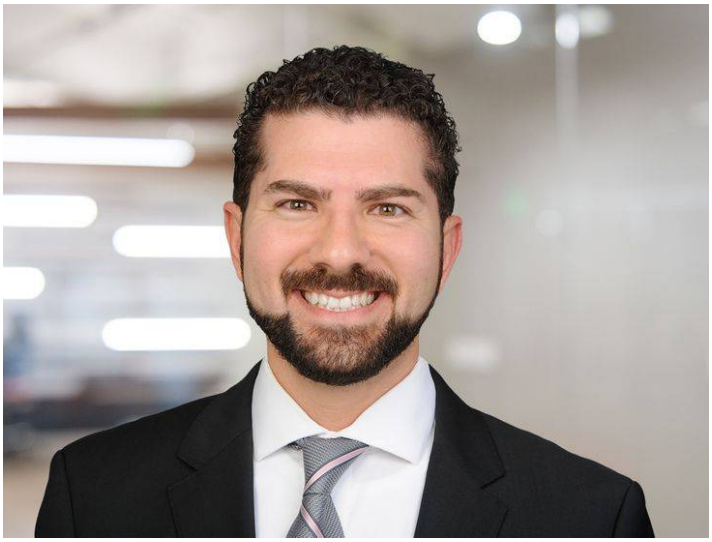
Follow FP's Digital Wiretapping Tracker: Closely monitor new and progressing privacy litigation claims to stay ahead of legal risk. To assist with this, Fisher Phillips has developed a Wiretapping Litigation Tracking Map to help businesses gain insight into legal trends by state, industry, and court jurisdiction. Understanding litigation trends can help you plan proactive measures that balance online business needs and consumer privacy expectations.

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 authors of this Insight, or any member of our Privacy and Cyber team.

Related People

Catherine M. Contino
Associate
610.230.6103
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills