# Federal Appeals Court Hands Out Win in Website Chat Wiretap Case: What It Means for Your Business

Insights
7.21.25

If your company uses a third-party tool to power your website chat function or AI-assisted customer service, the 9th Circuit Court of Appeals just delivered a ruling you should know about. On July 9, the court affirmed summary judgment for the defense in a high-profile privacy case brought against Converse – and made it significantly harder for plaintiffs to weaponize California's wiretap law (CIPA) against businesses that rely on modern digital tools. Here's what happened, why it matters, and what you should do next.

**The Case at a Glance**

In *Gutierrez v. Converse Inc.*, a website visitor claimed that Converse's use of a website chat vendor amounted to wiretapping in violation of the California Invasion of Privacy Act (CIPA). The plaintiff filed suit in California federal court, arguing that the third-party tech vendor intercepted and *potentially* read her chat communications – and that Converse should be held liable for aiding and abetting that violation.

But in last week's opinion, the 9th Circuit wasn't persuaded. It agreed with the lower court that granted Converse's motion for summary judgment for three main reasons:

- **No wiretap:** The court said there was no evidence the vendor made an unauthorized connection using a "telephone wire, line, cable, or instrument" as required for a violation of the first clause of CIPA Section 631(a).
- **No reading of messages:** Even if the vendor *could* access messages, there was no proof it *actually did* or actually attempted to do that – and that's a critical difference under the law. Mere capability or potentially being able to intercept and read a private communication is not the same as an interception and not enough to establish liability under the second clause of CIPA Section 631(a).
- **No aiding and abetting:** Because there was no underlying violation by the vendor, Converse couldn't be held secondarily liable.

**Why This Matters for Employers and Businesses**

- **It raises the bar for privacy lawsuits involving website chat tools.**

Under the standard set by this case, plaintiffs now need hard proof that a vendor actually intercepted or attempted to intercept and read a live message while in transit – not just that it *could* have or was capable of doing that. That's a significant evidentiary burden.

- **It calls into question CIPA's applicability to internet communications.**

A concurring judge argued that CIPA Section 631(a) – first written in 1967 – was never intended to apply to digital communications. He pointed out that the law was aimed at wiretapping telephones, not intercepting chat messages or web traffic. This observation is significant because plaintiffs' trend in privacy law is to attempt to revive old laws to establish claims applied to new technology.

- **It could ripple beyond chat features.**

The court's logic here could apply to AI-based customer service, voice assistants, and call-recording systems. Plaintiffs in lawsuits filed against AI vendors and their corporate customers for use of an AI tool to record, transcribe, summarize, or process incoming calls are already arguing that the vendor's mere capability of being able to access the data in real-time and mere potential or capability of using the contents of the recorded call to train their AI model is sufficient to establish a wiretapping claim. Defendants in such AI litigation will cite to this decision for the proposition that mere capability of accessing a private call is not enough under CIPA.

- **It may push plaintiffs to shift legal strategy.**

CIPA offers hefty statutory damages ($5,000 per violation). But if courts keep limiting its scope, plaintiffs may turn to laws like the California Consumer Privacy Act (CCPA), which focus on data misuse rather than message interception, as well as wiretapping laws in other two-party consent states and the Federal Wiretap Act.

**5 Practical Steps for Your Business**

**1. Review your third-party tools and vendors.**

Make sure you understand how your chat features, AI bots, and call center tools actually work – especially whether they *store* or *access* communications in transit.

**2. Ask the right technical questions.**

Even if a vendor *can* access a message, does it? If not, can you get written documentation or assurances to that effect? You might want to check out our detailed Insight: *The Essential Questions to Ask Your AI Vendor Before Deploying Artificial Intelligence at Your Organization*.

**3. Bolster your privacy disclosures.**

Review your privacy policy and other consumer disclosures and whether communications may be monitored, how they are processed, and whether vendors are involved.

**4. Track related legal developments.**

Several other CIPA cases are moving through the courts. Stay tuned for further rulings that could reinforce or undercut this decision. You can always be sure of getting the latest by subscribing to our FP Insight System.

**5. Prepare for plaintiffs to pivot to CCPA or other laws.**

CIPA may be narrowing, but CCPA, wiretapping laws in other states (such as Pennsylvania), the Federal Wiretap Act, and emerging AI privacy statutes are still in play. Make sure your compliance program doesn't rely on a single statute's safe harbor.

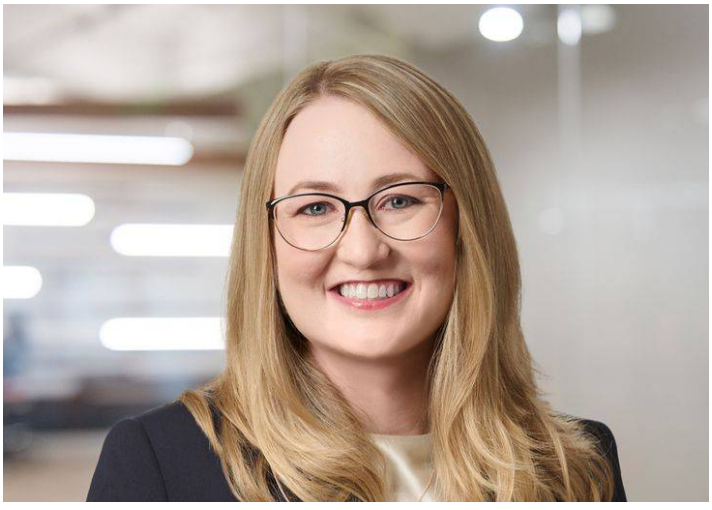
**What's Next?**

The 9th Circuit's ruling is the latest in a growing string of decisions limiting CIPA's use against internet-based communications – but it doesn't shut the door entirely. Plaintiffs are still testing new theories, especially as courts grapple with applying mid-century statutes to AI-enabled systems. However, by requiring proof of actual interception, not theoretical capability, the 9th Circuit gives businesses a clearer path forward, but also puts pressure on privacy teams to button up policies.

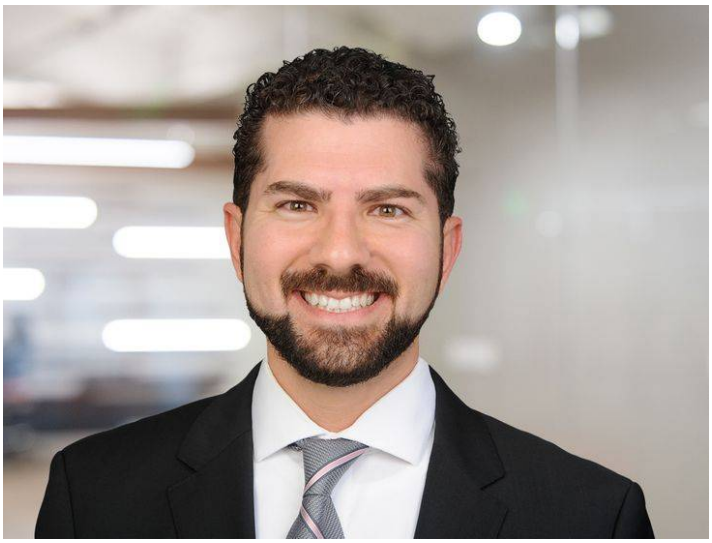
**Conclusion**

If you have any questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group or on our Privacy and Cyber team. Make sure you are subscribed to the Fisher Phillips' Insight System to receive the latest developments straight to your inbox.

## *Related People*



**Catherine M. Contino**
Associate
610.230.6103
Email



**Usama Kahf, CIPP/US**
Partner
949.798.2118
Email

**Danielle Kays**
Partner
312.260.4751
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