AI Call-Monitoring Lawsuits Are Heating Up: 5 Steps Your Business Can Take to Minimize Risk

Insights
6.18.25

A new lawsuit just filed against an AI software provider offers a clear warning for any business using artificial intelligence to monitor or record customer service calls. On June 13, a California plaintiff filed a federal class action complaint alleging that Cresta Intelligence, a provider of real-time AI conversation tools, violated the state's privacy law by capturing, analyzing, and storing her customer service call without her knowledge or consent. The lawsuit doesn't just target the *use* of call data but targets the vendor's mere *capability* to use that data for its own purposes, such as training AI models or developing new product features. And this is not an isolated case. Similar wiretapping lawsuits have been filed against major brands and their tech vendors, and courts are increasingly letting these cases proceed past early dismissal stages. What do you need to do to protect your business, and what are the five steps you can take to minimize risk?

 Join us at AI ADVANTAGE: An FP Conference for Business Leaders for a full discussion about AI litigation trends. Register now before the hotel block guarantee expires on June 27!

What's the Case About?

In *Galanter v. Cresta Intelligence*, a customer named Judy Galanter alleges that:

- She called a business from California to speak with a customer service agent.
- Without her knowledge, Cresta – an AI vendor retained by the business – recorded, transcribed, and analyzed the call using AI and natural language processing (NLP) tools.
- Cresta's platform is designed to learn from live calls and help train future models, generate business analytics, and improve product performance.

While Galanter admits she was told that her call may be "monitored or recorded for quality purposes," she claims there was no disclosure that her call would also be shared with a third-party AI system for purposes unrelated to quality assurance. The lawsuit claims the failure to disclose the usage of third-party AI violated the California Invasion of Privacy Act (CIPA), which prohibits recording or intercepting confidential communications without all-party consent.

Why This Matters to Your Business

This issue should be a growing compliance concern for any business using AI-driven voice analytics, chatbots, or customer engagement platforms. The legal risks ahead are daunting:

- **Third-party liability:** Even if your business isn't doing the recording, plaintiffs' counsel are asking courts to treat your AI vendor as an independent "eavesdropper" if it has the *capability* to use the data for its own commercial purposes regardless of whether it actually does. You might get dragged into the litigation under the theory that you aided and abetted this eavesdropper by implementing the AI technology.
- **Multiple states require all-party consent:** California's CIPA requires *all-party consent* to record conversations and applies to real-time monitoring – and other states also have all-party consent requirements.
- **Disclosures may fall short:** This case will test the theory of whether generic "this call may be monitored for quality purposes" notices cut it for legal purposes, especially when third-party AI tools are involved.
- **Claims might proceed without proof of harm:** Under the theory proposed by Galanter, courts would not need to require plaintiffs like her to provide evidence that AI vendors actually used the data at issue – just that they *could* have.

What's Next?

- Galanter will first seek to **expand her claim into a class action**, representing all California residents who called the business in question while in California and whose conversations were intercepted and recorded by Cresta. This number could reach into the tens of thousands.
- She is seeking to recover $5,000 per call under two separate provisions of CIPA, which could reach into the **hundreds of millions of dollars** (not to mention attorney fee recovery and other damages).
- Cresta has not yet filed any response to the lawsuit, as it was just filed several days ago, and will most likely defend the claims vigorously. It's important to remember that the **allegations discussed above are just that – allegations**. Cresta will have an opportunity to rebut the claims made by Galanter as the case proceeds.
- Regardless of what happens in the Cresta case, this issue will not go away. This lawsuit is just one of a **spate of new filings** that have been launched against AI providers and businesses in recent months as plaintiffs' attorneys test new theories and hope to identify new vulnerabilities.

What Should Your Business Do? 5 Steps to Minimize Risk

To minimize your legal exposure, especially in California, consider taking these five proactive steps:

1. Audit Your Vendor Relationships

- Know what third-party AI, analytics, or call software vendors you use to record calls, to provide real-time transcripts or analyses of calls, or which can otherwise be perceived as "listening" to calls.
- Review their privacy policies and user agreements – do they retain or use data to "improve services," or even just reserve the right to do so in the future?
- Read our valuable resource: **The Essential Questions to Ask Your AI Vendor Before Deploying Artificial Intelligence at Your Organization**

2. Strengthen Disclosures

- Update call center scripts, interactive voice response (IVR) prompts, and chatbot notices to explicitly state that third parties may access and analyze conversations.
- Don't rely on vague "quality assurance" language if data is also used to train AI or enhance vendor products.

3. Tighten Contracts

- Amend vendor agreements to limit data use strictly to your business purposes.
- Even if the law does not actually require that you do so, for the sake of avoiding or minimizing litigation risk, consider requiring AI vendors to confirm that data will not be reused for unrelated model training, analytics, or commercialization.

4. Monitor State Law Trends

- California is the current epicenter, but other states are watching closely. Similar lawsuits may spread, especially in jurisdictions with strong wiretapping laws.

5. Train Your Teams

- Make sure your privacy, legal, and customer support teams understand the compliance risks tied to AI tools, especially those involving voice and chat data.

Want to Learn More About AI Litigation?

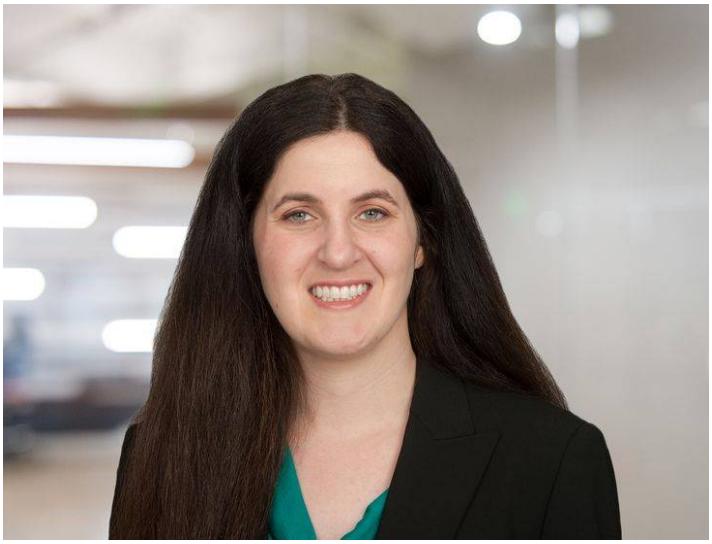
Join Fisher Phillips for our third-annual AI Conference for business professionals this July 23 to 25, in Washington, D.C. Learn more and register here.

Conclusion

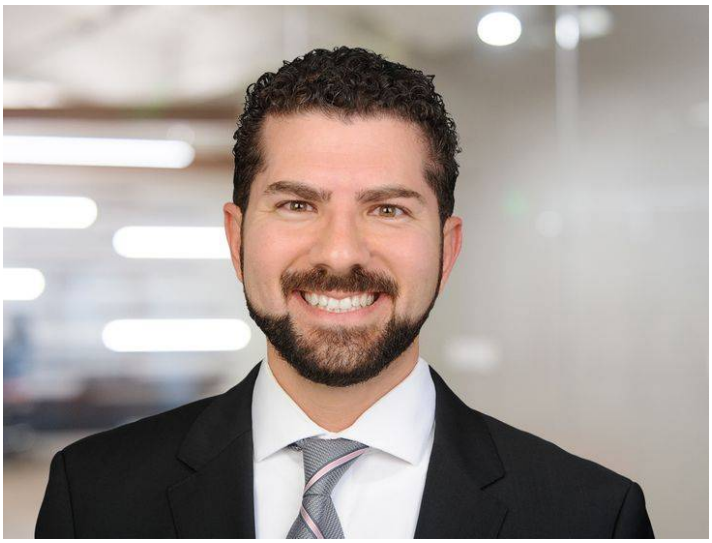
If you're using (or considering) these tools, now's the time to double-check your compliance posture. Contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI,

Data, and Analytics Practice Group, or Privacy and Cyber Team. And make sure you are subscribed to Fisher Phillips' Insight System to receive the latest developments straight to your inbox.

Related People



Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

AI, Data, and Analytics

Privacy and Cyber

Litigation and Trials

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills