New Lawsuit Highlights Concerns About AI Notetakers: 7 Steps Businesses Should Take

Insights 8.21.25

A new lawsuit just filed against Otter.ai underscores the legal and compliance risks companies face when using AI notetakers – and serves as a good reminder to deploy best practices to reduce your risks. The August 15 case alleges that Otter's popular transcription tool secretly records conversations without proper consent and then uses that data to train its machine-learning models. While AI notetakers can boost productivity, they also raise privacy, security, and compliance questions. This Insight reviews the lawsuit, goes over key risks, and outlines seven practical steps businesses should take before relying on AI transcription tools.

Case Summary: *Brewer v Otter.ai*

- **Court**: US District Court, Northern District of California (5:25-cv-06911)
- **Filed:** August 15
- **Judge:** Hon. Eumi K. Lee
- **Complaint:** Available by clicking here

The consumer filed a proposed class action in California federal court against Otter.ai, maker of the widely used Otter Notetaker. The complaint alleges the app unlawfully records conversations in popular video conferencing platforms without the consent of all participants.

Key allegations include:

- **Unauthorized interception of conversations:** The suit claims Otter records not only its account holder customers but also unsuspecting third parties involved in customer's meetings, allegedly violating federal and California wiretap laws.
- **Use of recordings to train AI models:** According to the complaint, Otter allegedly retains conversational data indefinitely and leverages it to refine its speech recognition technology without participant permission.
- **Shifting responsibility:** The lawsuit asserts that Otter tells its customers to "make sure you have the necessary permissions" – effectively outsourcing compliance obligations to customers rather than obtaining proper consent itself.
- **Violations of multiple laws:** The complaint includes claims under the federal Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), the California Invasion of Privacy Act (CIPA), and other privacy statutes, as well as common law privacy torts and the state's Unfair Competition Law.

Importantly, these are only allegations at early stages of the litigation. The complaint reflects the plaintiff's version of events only. Otter has not yet filed its response to the lawsuit, the court has not made any findings of fact or law, and the company will have an opportunity to contest and defend these claims in court.

The Real Risks with AI Notetakers

Let's be clear: we know you're going to use a notetaker app – we're not here to talk you out of it. And even if employers tell their employees not to use these tools, studies show employees are using them anyway. So cases like this highlight why employers need to proceed carefully. Common concerns include:

- **Consent and Privacy Laws:** Many jurisdictions require all parties to consent before recording conversations. You should review whether AI notetakers obtain consent from only the host or every participant.
- **Data Ownership and Use:** Unless you have an enterprise account or there are other contractual restrictions, review whether vendors retain recordings, transcripts, and even metadata indefinitely or use them to train AI models. Even when content is deleted, metadata about meetings often remains stored with the vendor. That means sensitive business information may influence how the model behaves, and in some cases could even be memorized and reproduced.
- **Security Vulnerabilities:** Consider whether recordings stored in the cloud are secure and properly protected.
- **Compliance with Workplace Laws:** Do conversations include legally protected discussions (e.g., about health conditions, union activity, or complaints of harassment). Recording and storing this content may raise risks.
- **Privilege and Confidentiality:** Whether notetakers may inadvertently capture attorney-client discussions or other privileged communications, raising questions about whether privilege can be maintained.
- **Reputational Exposure:** Even if legally defensible, employees or clients may perceive silent recording as a breach of trust.

7 Steps Businesses Can Take

If your organization is using or considering AI notetaker tools, here are seven proactive steps to manage risk:

1. Update Consent Protocols

- Obtain consent from all participants, including external parties, before using a notetaker. Consider the need to obtain this consent each and every time you deploy a notetaker.
- This is true whether your meeting is with external participants or solely an internal meeting. Ensure employees understand that meetings may be recorded or transcribed through the same consent procedures (and include notice in your internal company policies as an extra layer of protection).

2. Carefully Vet Your Vendors

- Ask direct questions about how data is stored, retained, and used for AI training.
- Seek contractual assurances that sensitive data won't be repurposed.
- Follow our guide to determine which questions to ask about notetakers and other AI usage.

3. Establish a Company Policy

- Provide policies that explain when and how AI notetakers may be used.
- Review employee responsibilities, including the notification to meeting participants, obtaining consent, and storage or deletion of recordings.

4. Limit Recording of Sensitive Conversations

- Review policies and protocols regarding AI notetaker use in meetings involving privileged, confidential, or sensitive HR topics.
- Consult with legal, compliance, or HR before deploying a notetaker in high-risk situations (like investigations, performance reviews, legal strategy discussions, and similar settings).

5. Review Security Safeguards

- Review vendors' use of encryption and strong access controls.
- Consider auditing where data is stored geographically and whether it is subject to cross-border transfer.

6. Train Employees and Managers

- Discuss with staff when appropriate (and when not) to deploy AI notetakers.
- Provide scripts for informing clients or third parties that a notetaker is in use.

7. Develop a Governance Framework

- Incorporate AI notetaker use into your broader AI governance strategy.
- Align practices with EEOC, FTC, and NIST guidance on AI tools to stay ahead of evolving regulations.
- Follow our AI Governance guide to develop your own protocols.