SEPTEMBER 3, 2025

Otter.ai Suit Highlights Risks of Using User Data to Train AI

by Meghan K. Farmer , Tatum Andres

Otter.ai is facing a federal class action in California alleging that its AI transcription tool, Otter Notetaker, secretly recorded private conversations on popular video conferencing platforms without proper consent. The tool provides real-time transcriptions for accountholders, but according to the complaint, it only seeks permission from the meeting host and even then, only if the host is not an Otter.ai user. Other participants cannot disable the tool, and if the host is an Otter.ai accountholder with an integrated account, the Notetaker can join meetings without any affirmative consent from attendees. The lawsuit further claims Otter used these recordings to train its speech recognition models, in violation of federal wiretap law and California privacy statutes.

The bottom line:
This case underscores the legal risks of using AI transcription tools and training AI on user data without clear, informed consent. Otter.ai's privacy policy claims it trains on "de-identified" recordings, but courts and regulators have been skeptical of such assurances. For example, a federal court in Illinois allowed BIPA claims to proceed where facial templates were created from images even without names attached, holding that the templates could still qualify as biometric identifiers. Regulators have also challenged anonymization claims when data could reasonably be re-linked to individuals, as seen in the FTC's 2021 settlement with Everalbum over facial recognition practices. As AI models increasingly rely on biometric, geolocation, and consumer behavior data, companies should expect heightened scrutiny.

What you need to do:
Companies developing or deploying AI-powered tools should carefully review how meeting data is collected and disclosed in privacy policies. Ensure consent is obtained from all participants, not just account holders. With respect to establishing use rights in data for AI training, avoid relying solely on de-identification. Updating product settings to provide notice and meaningful control can help reduce exposure to claims like those facing Otter.ai.
Questions? Our Privacy Team is available to assist: https://ktslaw.com/Services/CybersecurityPrivacyDataGovernance