

JANUARY 21, 2026 | PUBLICATION

"AI Notetakers in the Boardroom: Privilege and Privacy Considerations"

Businesses across many industries are racing to capture the value of artificial intelligence (AI) notetakers and meeting recording tools. The promise is obvious: faster follow-ups, searchable records, and fewer dropped threads. The legal implications are less obvious. The same software that multiplies efficiency also expands risks around privilege, privacy, and—if litigation ensues—discovery.

Picture this: you're in a meeting to discuss sensitive, confidential company strategy. A well-meaning manager arrives with a laptop, a cup of coffee, and a guest wearing a name tag that reads "Mr. Notetaker." Regardless of Mr. Notetaker's notetaking abilities, most stakeholders (or their attorneys) would probably ask who Mr. Notetaker is, and, upon learning he isn't affiliated with the company, politely ask him to leave before privileged discussion ends up in the hands of a third party not bound by any sort of confidentiality agreement.

AI notetakers and automatic transcription services are a digital version of "Mr. Notetaker." Unless they are deployed with proper controls, third-party problems remain.

Some tools also retain data for AI model training, analytics, and product improvement. In other words, the AI keeps the information you feed it.

A recent federal class action lawsuit in Illinois (Case No. 3:25-cv-03399-SEM-DJQ, *Cruz v. Fireflies.AI Corp.*) illustrates these concerns in the context of biometric data retention. The plaintiff alleges an AI meeting assistant that joins common videoconference platforms like Zoom, Teams, and Google Meet collects, possesses, and retains biometric data without proper notice, written consent, or observance of statutory safeguards. More specifically, the plaintiff alleges the software records, analyzes, transcribes, and stores voiceprints.

Functionally, voiceprints can be used to access restricted, personal, or otherwise confidential information.

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Andrew R. DeWeese

MEDIA CONTACT

Wendy M. Byrne

wbyrne@shumaker.com

For consumers (like the plaintiff in the Illinois lawsuit), unsecured voiceprints can increase the risk of identity theft or fraud. Similar concerns exist in the commercial context: authentication systems could be compromised if decision-makers lose control of their data.

Engagement letters with outside counsel, vendor data processing agreements, and explicit confidentiality provisions help demonstrate that AI tools are acting as agents rather than independent recipients. Enterprise-grade deployments of tools also typically offer “no-training” modes, on-premises or private cloud options, and contractual assurances that limit data use. The risk, however, doesn’t necessarily end there.

Even when AI-based scribes are deployed with sufficient confidentiality controls, outputs that are not subject to the attorney-client privilege could be discoverable in the event of litigation. Like traditional meeting minutes and notes, AI recordings and summaries may be requested by an opposing party in a lawsuit. Additionally, adding more “notetakers” generates more data subject to an organization’s data retention policies or formal legal hold notices.

Can AI notetakers streamline operations? Absolutely. Is there a point of diminishing returns? Quite possibly.

The difference lies in intentional deployment. Before making AI notetakers a mainstay in the boardroom, it’s worth considering diligence points such as data ingestion policies, default training settings, user isolation, encryption, access logging, role-based controls, deletion guarantees, and data privacy agreements that reflect an organization’s security standards and commitments.

The right answer will vary for every organization. To calibrate privilege, privacy, and discovery risks to your business needs, consider speaking with experienced data privacy and cybersecurity counsel.

Please contact Andrew DeWeese or a member of Shumaker’s Technology, Data Privacy, Cybersecurity & AI Service Line with questions or for more information.