Who's Really in the Room? Hidden Risks of AI Note-Takers

February 12, 2026

Pittsburgh, PA

TEQ Hub

(by **Jenn Malik** and **Peter Zittel**)

Most companies would never allow an unknown third party to sit in on executive level strategy sessions, legal consultations, or sensitive personnel discussions. Yet AI meeting assistants now perform a functional equivalent of that role, often without formal approval, policy guidance, or executive awareness. What may at first appear to be a simple productivity tool can, in practice, create significant legal and financial exposure. These AI meeting assistants are increasingly transforming ordinary business conversations into permanent, searchable data sets, in turn raising issues of privilege waiver, regulatory compliance, and potential litigation cost that many organizations have not yet confronted.

For business leaders, this realization raises an uncomfortable reality: what was assumed to be a confidential internal discussion may now exist as a permanent data record outside the organization's control.

In August 2025, similar circumstances gave rise to a nationwide class action lawsuit alleging that an AI meeting assistant unlawfully intercepted and recorded private video-conference meetings without obtaining consent from all participants. The plaintiffs in *Brewer v. Otter.ai* claim the AI tool joined meetings as an autonomous participant, transmitted conversations to third-party servers for transcription, recorded individuals who were not account holders, provided limited or unclear notice, and placed the burden of obtaining consent on meeting hosts. The lawsuit further alleges that recordings were retained indefinitely and used to train AI models, including the voices of individuals who were unaware they were being recorded. While the legal claims are still unfolding, the case underscores a broader and more immediate concern for business owners: AI meeting assistants can quietly convert everyday business conversations into legally consequential data assets, creating exposure well beyond what most organizations anticipate.

AI meeting assistants promise real benefits. They allow participants to stay engaged rather than take notes, generate meeting summaries and action items, promote consistency across teams, and even identify speakers automatically. For busy executives and businesspeople, these tools can feel indispensable. What is less obvious is that AI meeting assistants introduce a third party into conversations that have historically been governed by expectations of privacy, confidentiality, and limited retention. That shift has significant implications for attorney–client privilege, compliance with wiretap and privacy laws, and litigation exposure. From a business perspective, the issue is not whether these tools are useful, but whether they are being deployed with appropriate governance and risk awareness.

Attorney-Client Privilege

Attorney–client privilege is among the most powerful legal protections available to businesses. It shields confidential communications between lawyers and clients made for the purpose of obtaining or providing legal advice. However, that protection depends on confidentiality, and it can be waived through voluntary disclosure to third parties. Attorney–client privilege, which is held by the client, rests on four requirements: (1) there must be a communication, (2) made in confidence, (3) between privileged persons (lawyers and clients), (4) for the purpose of obtaining or providing legal advice.

AI meeting assistants are operated by third-party vendors. These tools typically route audio and text through external servers, and vendor terms of service often reserve rights to retain, access, or process the data. Even if no human listens to the recordings, the presence of an outside platform can undermine the confidentiality required for privilege to attach.

For business owners, the risk is apparent. Board meetings, executive strategy sessions, HR investigations, compliance reviews, and legal consultations increasingly occur over video platforms. Introducing an AI transcription tool into those conversations can create a credible argument that privileged communications were disclosed to a third party, weakening or eliminating the ability to shield them from discovery later. In short, convenience-driven use of AI meeting assistants can unintentionally expose the most sensitive communications a business has.

Wiretap Laws

AI meeting assistants also create risk under state and federal wiretap statutes, which regulate when audio recordings are lawful. While some states permit recording with consent from only one participant, others require consent from all participants. The distinction is critical. Remote work amplifies this risk. Virtual meetings often include participants located in multiple states, and businesses may not know where every attendee is physically located at the time of a call. Because wiretap laws generally focus on the speaker's location, the presence of even one participant in an all-party consent state can trigger heightened consent requirements for the entire meeting.

AI meeting assistants further complicate compliance because they do more than create a local recording. They transmit audio to third-party servers for processing, which may cause the AI provider itself to be treated as an intercepting party. Many platforms rely on vague or inconsistent disclosures that do not clearly explain who is recording, how the data will be used, or where it will be stored. Courts evaluating wiretap claims often require knowing and voluntary consent, and passive or unclear notice may not satisfy that standard.

For businesses, this means wiretap exposure can arise without bad intent, simply because an AI assistant was enabled by default or added to a call without affirmative consent from all participants.

Privacy Laws

Many AI meeting platforms acknowledge, often in dense privacy policies, that recorded conversations may be retained and used to train speech-recognition or generative AI models. What begins as a routine business meeting can therefore become part of a long-term dataset used for purposes unrelated to the original discussion. From a business perspective, the most underappreciated risk is loss of control. Voices, speech patterns, job titles, project references, and contextual details can make so-called "de-identified" data traceable back to individuals or organizations. Once recordings are incorporated into training pipelines, deletion may be difficult or impossible.

This practice raises serious concerns under a range of privacy regimes. Healthcare-related discussions may implicate HIPAA restrictions. International operations may trigger GDPR obligations related to purpose limitation, data minimization, and deletion rights. Even California's privacy laws grant individuals enhanced rights to transparency and restrictions on secondary uses of their data, including undisclosed AI training.

Discovery Exposure

AI-generated transcripts also carry significant litigation risk. Unlike traditional handwritten notes or informal summaries, AI transcripts are permanent, detailed, searchable, and time-stamped. In litigation, these records can become prime discovery targets. Opposing counsel may seek years of internal meeting transcripts, searching for statements taken out of context or distorted by transcription errors. The existence of extensive AI-generated records can materially increase legal expenditures, expand discovery disputes, and weaken negotiating leverage, often regardless of the merits of the underlying claims. What begins as a productivity tool can, in practice, create a vast and expensive new category of discoverable material.

Conclusion

AI meeting assistants are not merely efficiency tools; they fundamentally alter how business conversations are captured, stored, and regulated. By converting human speech into portable and persistent data assets, these platforms can trigger privilege waivers, wiretap violations, privacy compliance obligations, and expanded discovery exposure, often without any deliberate decision by business leadership.

The lesson is not that businesses should abandon AI innovation. Rather, they must recognize that these tools require governance. Privileged legal communications should remain free from third-party transcription. Outside that context, organizations should implement clear policies governing when AI meeting assistants may be used, how consent is obtained, how data is retained or deleted, and which meetings are categorically off-limits.

Until legislatures and courts provide clearer guidance, the burden rests squarely on organizations to manage these risks. In some high-stakes settings, the most compliant option may remain the simplest one: keep AI out of the meeting entirely. Convenience may sell AI meeting assistants, but governance is what prevents convenience from becoming liability.

Jenn L. Malik is a shareholder in the firm's Corporate and Commercial, Employment and Labor, and Public Sector groups, focusing her practice on healthcare benefits, data privacy, insurance coverage, and appellate law. Contact her at 412-394-5490 or jmalik@babstcalland.com.

Peter D. Zittel is an associate at the firm, focusing his practice primarily on municipal and land use law. Contact him at 412-773-8711 or pzittel@babstcalland.com.

To view the full article, **click here**.