Eavesdropping by Algorithm: Legal Risks of AI Meeting Assistants

December 24, 2025

Pittsburgh, PA

The Legal Intelligencer

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

Imagine sitting down for a virtual meeting where sensitive legal matters are being discussed and internal strategy decisions are unfolding, with everyone assuming the conversation is confidential and limited to the people on the call. Only later does someone in the meeting realize that a small “note-taker” icon was glowing in the corner of the screen, an artificial intelligence tool was present, recording and transcribing every word that was said. In that moment, the participants realize that what they assumed was a confidential discussion may indeed, not be so private.

These are the exact events that resulted in the filing of a nationwide class action in August 2025. In *Brewer v. Otter.ai* , plaintiffs allege that Otter.ai’s “Notetaker” and “OtterPilot” tools unlawfully intercepted and recorded private video-conference meetings without obtaining consent from all participants. The complaint claims the AI assistant joins calls as an autonomous participant, transmits conversations to Otter’s servers for transcription, records even non-account holders, provides little or no participant notice, and shifts responsibility for consent onto meeting hosts. Plaintiffs further allege Otter retained recordings indefinitely and used captured communications to train its AI models, including voices of individuals who were unaware they were being recorded. The lawsuit asserts federal wiretap and computer-access violations, multiple California privacy law violations, and common-law claims for intrusion and conversion, casting AI notetakers not as neutral productivity tools but as unauthorized third-party surveillance operating inside private meetings.

AI meeting assistants offer numerous benefits, including allowing participants who would otherwise be taking notes to stay fully engaged, automatically generating meeting summaries and action items, producing uniform and unbiased notes for all participants, and even identifying speakers by their voices. But what many users do not fully appreciate is that these tools introduce a third party into conversations historically governed by strict privacy and confidentiality rules, a shift that carries profound consequences for attorney–client privilege, wiretap compliance, compliance with privacy laws, Pennsylvania’s Right to Know Law (“RTKL”), and discovery exposure.

1. **Attorney-Client Privilege**
   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. That protection is incredibly powerful, preventing discovery of sensitive conversations even in the midst of intense litigation. However, the privilege can be waived through voluntary disclosure to third parties, and AI transcription tools are owned by third parties. These AI meeting assistant tools typically route audio and text through third-party servers or cloud-based servers, and even if no employee actively “listens,” the vendors often retain access rights under their terms of service, storage practices, or model-training procedures to the information disclosed. As people increasingly rely on these tools to summarize privileged meetings, process attorney emails, or analyze legal memoranda, they are placing sensitive communications into systems operated by outside vendors, and consequently, could be waiving attorney-client privilege. Additionally, many of these vendors may log inputs, retain data, or use uploaded content to improve their AI models. Introducing an AI platform into a legal discussion under these conditions can undermine the confidentiality required for privilege to attach and may severely weaken any later claim that the communications were intended to remain private.

2. **Wiretap Laws**
   AI meeting assistants may also run afoul of state and federal wiretap statutes. Generally, wiretapping statutes regulate when recording is lawful, and the core requirement is consent. Some states permit recording with consent from only one participant, while others require all participants to agree. That distinction is critical: a lawful recording in a one-party consent state may become illegal if even a single participant joins from an all-party consent jurisdiction.

   Remote work amplifies this problem. Virtual meetings routinely include participants located across multiple states, often without anyone knowing where other attendees are physically calling in from. Because wiretap laws generally focus on the speaker's location, the presence of just 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 are not simple local recordings. They transmit audio to third-party servers for processing, which means the AI provider itself may be deemed an intercepting party. Many platforms rely on vague, optional, or inconsistent disclosures that fail to clearly explain who is recording, where data is sent, or how it will be used. Courts applying wiretap laws require knowing and voluntary consent, and these weak notices may not satisfy that standard, leaving organizations exposed to wiretap liability when participants never affirmatively agreed to third-party recording.

3. **Privacy Laws**
   Several AI meeting platforms acknowledge, often buried in privacy policies, that recorded conversations may be retained and used to train speech-recognition and generative AI models. What begins as a routine business meeting can therefore become a permanent training dataset outside the control of the speakers. Although vendors describe this data as "de-identified," true anonymization is difficult: voices, speech patterns, job titles, project references, geographic markers, and health or employment details can readily link recordings back to individuals. Once content enters training pipelines, deletion is usually impractical, converting what participants assumed was a fleeting exchange into a lasting data asset.

   The practice runs afoul of many privacy laws. HIPAA severely restricts disclosures tied to patient health information and limits even permitted disclosures to the minimum necessary required to achieve the intended purpose of the disclosure. The GDPR requires narrow purpose limitation, data minimization, and enforceable rights of access and deletion, standards difficult to reconcile with open-ended AI training uses. California's consumer privacy laws further heighten risk by granting individuals rights to transparency, restrictions on data processing, and challenges to undisclosed secondary uses such as model training. As a result, a single unnoticed recording can escalate from a brief compliance lapse into ongoing multi-regulatory exposure, with regulatory, litigation, and class-action consequences.

4. **Pennsylvania's RTKL**
   For Pennsylvania government agencies, AI meeting assistants present an additional and often overlooked risk under the RTKL. The RTKL broadly defines "records" to include any information documenting the transaction or activity of an agency, regardless of format. When an AI assistant generates verbatim transcripts of meetings involving municipal officials, staff, or boards, those transcripts may constitute public records subject to disclosure, even if no written minutes were otherwise required or intended to exist. Traditional meeting notes or informal recollections are limited and often transient, but AI transcripts create fixed, searchable, and highly detailed records that can be requested by any member of the public. This dramatically expands the volume of potentially responsive materials municipalities may have to review, redact, and produce. It also increases the risk that preliminary discussions, off-the-cuff remarks, or partially formed deliberations may become accessible through RTKL requests. Once created, these transcripts cannot easily be undone, and municipal agencies could find themselves responsible for preserving and disclosing extensive datasets that carry both administrative cost and legal risk, especially when multiple transcripts span years of internal meetings, planning sessions, or executive discussions.

5. **Discovery Exposure**
   For similar reasons as those enunciated above with respect to the RTKL, discovery risk also increases dramatically when meetings are recorded by default because AI transcripts differ fundamentally from traditional human notes. While handwritten or typed summaries are selective, imperfect, and often discarded, AI-generated transcripts are permanent, detailed, searchable, and time-stamped, making them powerful litigation targets. In

lawsuits, opposing counsel can demand production of entire datasets documenting years of internal corporate communications, combing transcripts for statements taken out of context or distorted by transcription errors to use in depositions and motion practice. What begins as a tool meant to improve productivity can, in practice, create vast new discovery burden and sharply increase litigation costs.

Conclusion

Collectively, these risks reveal a sobering reality, that AI notetakers convert private human speech into portable, persistent data assets that can trigger legal ramifications far more complex than most organizations realize. The rise of AI meeting assistants is not simply a question of workplace efficiency, it is a fundamental shift in how conversations are captured, stored, and regulated.

However, the lesson here is not to abandon the innovation that AI brings to the workplace but to acknowledge its legal consequences. Privileged attorney/client communications require the highest degree of confidentiality and should remain free from third-party transcription entirely. Outside the privilege context, organizations must nonetheless recognize that AI-generated transcripts can trigger wiretapping statutes, create new public-record obligations, broaden discovery exposure, and generate ongoing privacy compliance duties that far exceed typical internal note-taking practices.

Until legislatures and courts provide clearer guidance on how legal protections apply to artificial intelligence in real time communications, the burden rests squarely on organizations to govern these tools. AI notetaking programs should be subject to targeted policies, restricted use cases, robust oversight, and strict deletion practices. In high-risk settings, the most compliant option may remain the most straightforward one: keep AI out of the meeting entirely.

Convenience may be what sells 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, administration, 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**.