FOCUS: ARTIFICIAL INTELLIGENCE

Data Security and AI Transcription: Who's Really in on the Conversation?

Steven J. Kuperschmid and Rachel A. Morgenstern

Business owners across the globe are using the latest AI technology to increase efficiency in the workplace. From automated data analysis and chatbots to the more commonplace digital assistant, AI is practically everywhere and growing more versatile by the day.

Perhaps most popular among these new tools is AI transcription, now offered as a feature of most videoconferencing platforms, such as Zoom and Microsoft Teams. As with any new technology, however, AI transcription is not without risks, and for businesses that deal in sensitive or confidential information, it is especially important to consider taking precautions to mitigate those risks.

First, there is the risk of a privacy breach. The level of privacy concern at issue depends in large part on the type of user and the subject matter of the transcription. For instance, disclosure of the transcripts of an administrative meeting of an accounting firm where identifiable client information and proprietary firm practices are not discussed may not raise any significant privacy concerns. By contrast, disclosure of the transcript from a confidential meeting of a public company contemplating a merger might raise serious privacy concerns.

In addition to the risk of a security breach, there is the fact that documents, electronic and otherwise, can become public during litigation. By using AI transcription for confidential meetings, a business is creating a producible record of an event where previously none existed. If that business later becomes part of a litigation, those records may become public as part of discovery. The records may also be subject to the Court's subpoena power, even where the business itself is not a party to the litigation.

Second, there is the risk of error. All AI language models produce, at least to some degree, "hallucinations," which yield incorrect or misleading results. In this context, a hallucination might take the form of a meeting recap wherein one or two small details are incorrect. In other words, where an AI tool did not hear what someone said at a given point during the meeting, it would simply make something up. As a result, the user must weigh the risks and benefits of employing an inherently flawed technology. In October 2024, for instance, the Associated Press reported that certain hospitals were relying on an AI transcription product that deletes the original audio, leaving doctors with no means to check the transcriptions for errors afterwards, even though the model was known to produce hallucinations.[1]

Third, there is the risk of (at least alleged) waiver of attorney-client privilege. In March 2021, even before the launch of ChatGPT, the American Bar Association ("ABA") issued Formal Opinion 498, wherein it advised attorneys to shut off their phones during attorney-client discussions.[2] Specifically, the ABA said "[u]nless the technology is assisting the lawyer's law practice, the lawyer should disable the listening capability of the devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters. Otherwise, the lawyer is exposing the client's and other sensitive information to unnecessary and unauthorized third parties and increasing the risk of hacking."[3]

While U.S. courts have yet to decide a case based on allegations that AI caused a breach in attorney-client privilege, the ABA's concerns are not unfounded. Attorney-client privilege itself is rooted in the reasonable expectation that communications between a lawyer and his client will remain confidential. Where disclosure to a third party is inadvertent, the courts will often protect the privilege nonetheless. But if disclosure is voluntary, as it would be where either a lawyer or his client was using artificial intelligence to communicate, record, or transcribe, the courts would more likely deem the privilege waived.

Fourth, there is the risk of running afoul of two-party consent laws. New York is a one-party consent state, meaning as long as (1) all parties to the conversation are located in New York, and (2) one party consents to the recording, it is legal to record a conversation. When one of the parties is out-of-state, however, the analysis is more complicated.

There are several ways to address this issue. With some platforms, like Zoom, the host can require consent from all meeting participants before the recording begins. Another option is for the host to verbally announce his intentions to record or transcribe the call before recording begins. Ultimately, however, the responsibility for ensuring consent is obtained rests with the user. Zoom's terms of service provide, for example, that "[y]ou are responsible for compliance with all Laws governing the monitoring or recording of conversations" and "[y]ou will receive a notification (visual or otherwise) when recording is enabled."[4]

If the host announces that the call is being recorded, it is arguable that those participants who stay on the call have implicitly consented. Those who do not wish to be recorded have the option to drop off the call or, alternatively, to disable their video and mute themselves. As discussed further below, however, a "muted" user is not always unheard, as least by the AI.

While there is no disputing that generative AI has incredible potential as a business tool, some of the above-cited potential pitfalls have already become a reality. In October 2024, researcher and engineer Alex Bilzerian told the *Washington Post* that, after a Zoom meeting with some venture capitalist investors, he got an automated email from Otter.ai containing a transcript of the meeting, including the part that happened after he logged off (when the investors discussed their firm's strategic failures and cooked metrics).[5]

That same *Post* article discussed Otter.ai's "Otter Pilot," which records and transcribes audio from virtual meetings.[6] If an Otter Pilot user is muted, his audio will not be recorded, but if that muted user manually hits record, Otter receives audio from his microphone and speakers.[7] In other words, Otter hears what the "muted" user is saying.[8] The *Post* also discussed privacy concerns arising from the fact that "Otter shares user information with third parties, including AI services that provide back-end support for Otter, advertising partners and law enforcement agencies when required."[9]

When approached about the Bilzerian incident, discussed above, Otter responded by saying that users have the option to not share transcripts automatically with anyone or to auto-share conversations.[10] This response is typical of AI proponents, and represents the sentiment that AI is here to stay, and better combated by learning how to use it as safely as possible (and teaching employees to do the same), rather than trying to eradicate it entirely from one's business practice. In other words, the best defense might be to issue policies and guidance on the use of these tools in the workplace, and to enforce them strictly.

By taking certain basic precautions, business owners can minimize the potential risks associated with AI transcription. For instance, while many videoconferencing platforms are now offering AI transcription as an automatic feature, the user can often opt-out of automation. By choosing whether to transcribe on a case-by-case basis, the business can mitigate against having to produce sensitive or confidential information as part of litigation. As another example, those who are regularly using AI tools for transcription should employ a second level of review by company personnel as a matter of course. Make sure personnel are on the lookout for "hallucinations." Avoid relying on AI transcription for high-level issues where accuracy of content is paramount.

As AI continues to permeate other business applications, these types of precautions will run hand in hand with development of AI guidance and policies for employees and intensive employee training.

1. Garance Burke and Hilke Schellmann, *Researchers say an AI-powered transcription tool used in hospitals invents things no one ever said*, APNews, Oct. 26, 2024, https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14.
2. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498 (2024).
3. *Id.*
4. Zoom Terms of Service, Aug. 11, 2023, https://www.zoom.com/en/trust/terms/.
5. Tatum Hunter and Danielle Abril, *AI assistants are blabbing our embarrassing work secrets*, Oct. 2, 2024, https://www.washingtonpost.com/business/2024/10/02/ai-assistant-transcription-work-secrets-meetings/.
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*

Steven J. Kuperschmid serves as Co-Chair of Ruskin Moscou Faltischek, P.C.'s Corporate & Securities Department, Chair of the firm's Cybersecurity and Data Privacy Practice Group, and a member of the Blockchain Technology and Digital Asset Practice Group. He typically represents entrepreneurs, family businesses and publicly traded and privately owned institutional companies and private equity funds. He can be reached at skuperschmid@rmfpc.com.

Rachel Morgenstern is an Associate at Ruskin Moscou Faltischek, P.C., where she is a member of the firm's Estate, Trust and Fiduciary Litigation Practice Group, Commercial Litigation Department, Employment Practice Group, Fine Art Law Practice Group and the Insurance & Reinsurance Litigation, Dispute Resolution, Transactions, and Regulatory Problem Solving Practice group. She can be reached at rmorgenstern@rmfpc.com.