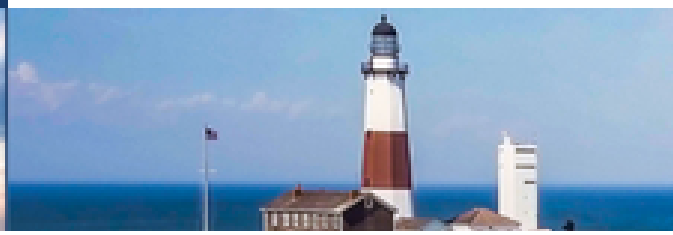
CYBERSECURITY LAW ALERT

April 23, 2025

By: Steven J. Kuperschmid, Esq.
Rachel A. Morgenstern, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.



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

Business owners across the globe are using the latest in AI technology to increase efficiency in the workplace. From automated data analysis and chat bots 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.

Risks and Precautions

- **Privacy breach.** Generally speaking, AI companies store data, such as AI transcripts, on external servers. While those companies are likely to use reasonable security measures in protecting that data, no security is invulnerable. In other words, there is at least some degree of exposure.
    - Precautions: The level of privacy concern at issue depends in large part on the type of user and the subject matter of the transcript. Where sensitive subject matters are being discussed, avoid using AI transcription and other AI technology.
- **Error.** All AI language models produce "hallucinations," which are incorrect or misleading results. In the context of transcription, a hallucination might take the form of a meeting recap wherein one or two facts are stated incorrectly. While some hallucinations are easy to identify, others can be difficult to detect. AI also still has trouble transcribing people with accents, and translating idiomatic expressions.
    - Precautions: 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.
- **Consent.** The laws about consent to record another person vary from state to state. 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 party is out-of-state, however, the analysis is more complicated. Ultimately, the person transcribing the call (or "host" of the videoconference, as it may be) is responsible for obtaining consent.

- Precautions: If the videoconferencing platform offers the option, require consent from all meeting participants before the recording begins. Otherwise, the host may verbally announce his intentions to record or transcribe the call before recording begins.

- **Subpoena Power.** 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.

  - Precautions: 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.

- **Attorney-Client Privilege.** There is a reasonable expectation that communications between a lawyer and his client will remain confidential. Where a client voluntarily discloses those communications to a third party, he may waive that privilege. This may include instances where a client voluntarily discloses those communications to third-party AI companies, though this theory has yet to be tested in U.S. courts.

  - Precautions: Never transcribe a conversation with an attorney.

By taking these basic precautions, business owners can minimize the potential risks associated with AI transcription. As AI continues to permeate other business applications, these precautions will run hand in hand with development of AI guidance and policies for employees and intensive employee training.

If you have any questions or if you would like to set up a meeting or a call to discuss how RMF can assist you with your practice, please reach out to:

Steven J. Kuperschmid, Esq.
516.663.6686
skuperschmid@rmfpc.com

Rachel A. Morgenstern, Esq.
516.663.6537
rmorgenstern@rmfpc.com