GOODWIN

APRIL 27, 2026

AI Transcription Tools Under Scrutiny: Navigating Privacy Risks and Practical Mitigation Strategies

Kaitlin Betancourt, Jacqueline Klosek, Rebecca Tarneja, Jacob T. Lee, Aaminah Bhat, Reema Moussa

The past few years have seen a wide variety of AI-powered innovations which have transformed the workplace. Of these tools, AI-powered automated transcription and note-taking technologies have become some of the most prevalent. These tools, which include meeting note-takers and “AI scribe” technologies, function by listening to attendee conversations and transcribing or summarizing those conversations into searchable text. While these tools have enhanced meeting efficiency and the reliability of note-taking, they have also created new risk vectors for organizations when leveraged without due care.

The Privacy Landscape: Why AI Transcription Tools Matter

AI scribes are often embedded in conferencing platforms that are commonplace. They can also be deployed as autonomous bots that join meetings, capture audio, and produce transcripts, summaries, or action items. Because these tools typically process audio streams in the cloud and involve third-party vendors, they raise privacy questions that extend beyond traditional note-taking. Transcribed conversations are durable, searchable, and often stored indefinitely, features that benefit productivity but also create a permanent, detailed record of what was said. Unlike informal handwritten notes, these records can be subject to legal discovery, regulatory disclosure requests, and privacy claims if not governed properly.

Privacy Legal Risks

Biometric Data Collection and Voiceprints

Certain AI transcription tools analyze voices, including, in some cases, to attribute speech to particular individuals. Where these systems process voice characteristics, such as pitch or vocal patterns, and use those characteristics to identify an individual, they may generate “voiceprints” which are subject to regulation, including, of most concern, US state biometric data laws. Notably, in 2025 and 2026, a number of companies have faced litigation under the Illinois Biometric Information Privacy Act (BIPA) for the above practices. In these cases, plaintiffs alleged that the tools created and stored their voiceprints without providing them with notice of collection or obtaining their consent as required under BIPA. The recent prevalence of these BIPA lawsuits underscores the risk of statutory damages and class action claims to which organizations and their vendors may be exposed tool if these tools are used on individuals without obtaining the individuals' consent.

Wiretapping and Electronic Recording Laws

Similarly, organizations and vendors that leverage AI transcription tools have also faced liability under US state and federal wiretap laws, which courts have found apply to the interception and recording of communications. While the use of these technologies arguably does not run afoul of wiretapping laws in one-party consent states, certain other states, including California, Florida, Illinois, and Massachusetts, require all parties to consent to recording. In all-party consent states, AI transcription tools that automatically join meetings or record audio without obtaining explicit advance consent from attendees through an opt-in or opt-out banner or other consent mechanism risk being found to have violated these statutes. Further, courts have found liability to arise under the federal wiretap laws and other one-party consent statutes under statutory exceptions, regardless of the organization's consent — such that organizations are at risk of claims under all US jurisdictions. Failing to comply with these wiretap laws may expose organizations and their vendors to civil liability under federal and state wiretapping statutes. For example, violations of the California Invasion of Privacy Act can result in organizations facing damages of up to $5,000 per violation. Additional exposure includes class action litigation, statutory computer fraud claims, common law claims including for invasion of privacy and intrusion upon seclusion, and, in the most egregious cases, criminal penalties.

Accuracy, Misinterpretation, and Automated Decision-Making

AI transcription technologies are not infallible. They can misidentify speakers, mischaracterize speaker intent, misinterpret jargon, and produce transcripts that differ from what was actually said. These inaccuracies can lead to privacy or legal disputes when transcripts are relied upon in litigation, investigations, or regulatory compliance. Furthermore, AI tools that generate summaries or action item lists may inadvertently introduce statements that were never spoken, further complicating the evidentiary reliability of records.

Moreover, reliance on AI transcription tools for certain decisions, such as revisiting an employee's annual performance review or other meetings that may result in significant decisions being made about an individual, may trigger liability under certain laws including US state privacy and AI governance laws. For example, recent amendments to the California Consumer Privacy Act (CCPA), effective January 1, 2027, require that companies relying on transcription tools to make decisions about an individual must give notice to consumers of this use, allow them to opt out of such processing, and respond to consumer access requests regarding the technology. Businesses that deploy these tools must also engage in privacy risk assessments where processing poses a significant risk to the consumer's privacy.

Attorney-Client Privilege and Confidentiality Risks

As discussed in a recent Goodwin Client Alert, the use of these tools can raise attorney-client privilege and confidentiality risks. Attorney-client privilege is generally destroyed by voluntary disclosure of privileged communications to third parties. Whether an AI transcription vendor qualifies as a functional equivalent of a legal assistant or stenographer, thereby preserving privilege, is an unsettled question of law. The privilege risk is not limited to law firms or outside counsel. In-house legal teams, companies involved in investigations, and executives in board strategy discussions attended by counsel are all equally at risk. In cross-border contexts, privilege standards may differ, further complicating risk assessments where transcripts are stored or processed outside the United States. Further, AI transcription tools used during legal consultations, investigations, or routine counseling may not qualify for attorney-client privilege and work-product protections in some circumstances, such as where the content or communications in question are prompted by a client,

rather than counsel.[1]

In addition, AI-generated transcripts convert oral discussions into durable, searchable records. Even where privilege ultimately applies, the existence of transcripts may expand the volume of materials subject to discovery and increase review burdens in litigation.

Data Retention, Vendor Use, and Cross-Border Risks

Once audio data and transcripts are generated, they often reside on systems controlled by the service provider, not the organization that initiated the recording. Depending on applicable license terms, these vendors may retain data indefinitely, share it with third parties, or use it for model training. These practices can run afoul of privacy laws — such as the CCPA or similar international regimes, which require transparen data practices and user rights regarding deletion, access, and opt-out — and give rise to additional privacy claims in litigation.

This risk is especially prevalent in regulated industries, such as healthcare. In these industries, failing to execute or update proper business associate agreements (BAAs) or data protection addendums (DPAs) with service providers that have access to consumer health data can expose organizations to HIPAA compliance risks or compliance risk under US state frameworks, such as Washington's My Health My Data Act if protected health information or consumer health data is processed without these contractual safeguards. The magnitude of this risk has been reflected in recent healthcare litigation that has alleged violations of such laws where clinical encounters have been recorded without proper authorization.

Risk Mitigation Strategies

While material privacy and litigation risks can arise from the use of AI transcription tools, organizations can deploy a range of strategies to mitigate legal exposure and responsibly integrate AI scribes into their workflows.

Comprehensive Consent Practices

Before activating an AI transcription tool, organizations should clearly disclose that transcription or recording will occur and obtain explicit, opt-in consent from all participants, whether employees or outside participants, before beginning any recording or transcription. In all-party consent states, the platform or workflow is responsible for enforcing these requirements and ensuring that adequate consent is obtained.

Vendor Due Diligence and Contractual Safeguards

Organizations should assess their selected AI transcription tool vendors for privacy and security practices, including, but not limited to:

- Data handling, retention, and deletion policies
- Policies related to the use of collected data for model training and/or third-party sharing
- Encryption standards and access controls
- Ability to execute contractual protections such as BAAs or DPAs where regulated information (e.g., protected health information or consumer health data) or consumer personal data is involved

Contracts should also require that vendors delete data upon request, restrict secondary use for training

without consent, and provide audit rights for compliance verification. Vendors that store or process data in foreign jurisdictions may also introduce cross-border privacy compliance complexities that should be addressed contractually.

Governance and Usage Policies

Establish formal governance policies that prescribe:

- Who is authorized to deploy AI transcription tools and what tools are permitted (externally deployed tools versus enterprise tools, for example)
- The importance of validating transcription outputs through employee review
- Consent protocols and retention policies
- What types of meetings or content are permitted to be transcribed by AI tools and, conversely, situations in which AI transcription tools are *prohibited*, such as privileged discussions with legal counsel, sensitive negotiations, or other high-risk contexts, including HR or legal matters
- Employee policies and mandatory employee training on the policies to mitigate the risk of claims arising from employees' use of transcription.

These policies should be integrated within an overarching AI governance framework, which should be aligned with the organization's privacy and information security frameworks. The AI governance framework should include approval mechanisms for new AI use case deployments and regular reviews of tools used.

Human Oversight and Accuracy Assurance

AI transcripts should not be treated as authoritative legal records without human review. Requiring human quality checks shortly after a given meeting takes place helps ensure accuracy, correct misattributions, and confirms that sensitive information has been handled appropriately. This review process also reduces risks associated with misinterpretations or omitted context.

Retention Limits and Legal Holds

AI transcription outputs should be governed by retention policies aligned with legal hold obligations and exemption requirements. Organizations should integrate AI transcript records into their records management systems and ensure that data is preserved when required for litigation, investigations, or regulatory audits, while also deleting obsolete data according to policy.

* * *

AI transcription tools can unlock productivity gains and enrich organizational knowledge flows. However, they also introduce consequential risks to privacy, confidentiality, privilege, intellectual property, and other sources of legal or operational risk. From potential BIPA violations over biometric data to wiretapping claims and privileged information exposure, recent lawsuits and evolving regulatory scrutiny reflect how these once-novel technologies are being tested in the legal and legislative arenas. To benefit from the use of AI transcription tools, organizations should adopt comprehensive consent practices, carefully vet vendors, establish governance policies, and preserve human oversight of transcripts. By implementing structured risk mitigation strategies, organizations can benefit from automation while safeguarding privacy, confidentiality, and compliance.

[1] See *United States v. Heppner* (Southern District of New York, 2026). Goodwin has also discussed this case here.

This informational piece, which may be considered advertising under the ethical rules of certain jurisdictions, is provided on the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin or its lawyers. Prior results do not guarantee similar outcomes.

CONTACTS

Kaitlin Betancourt
Partner
Data, Privacy & Cybersecurity
kbetancourt@goodwinlaw.com

Jacqueline Klosek
Partner
Strategic Technology Transactions and Licensing
jklosek@goodwinlaw.com

Rebecca Tarneja
Counsel
Complex Litigation & Dispute Resolution
rtarneja@goodwinlaw.com

Jacob T. Lee
Associate
Data, Privacy & Cybersecurity
jacoblee@goodwinlaw.com

Aaminah Bhat
Associate
Artificial Intelligence
abhat@goodwinlaw.com

Reema Moussa
Associate
rmoussa@goodwinlaw.com