

Justice Impact Briefing

Risks Associated with the Use of AI Transcription Tools and Notetaking Apps in Legal Proceedings

By: Jeopardizing Justice Coalition (jeopardizingjustice.com)



Introduction

It's no secret that we are in the midst of an Artificial Intelligence arms race. Tech companies are jockeying for position in all facets of day-to-day life as they tout their efficiency and superiority over one another without considering some of the impacts and repercussions in individual segments of society. As private industries and public sectors all over the world consider their options, from chatbots to air traffic control to healthcare systems to court proceedings, regulators and business leaders must consider multiple concerning factors in AI adoption.

Governments and lawmakers especially are tasked not only with conducting important public services in the most efficient and cost-effective way possible; they are also entrusted with safeguarding the privacy and security of their citizens' and constituents' information. For that reason, administrators and policymakers across the world are scrambling to meet the AI moment by establishing committees, task forces, and work groups to address these concerns, and we're starting to see the first drafts of regulations and guidelines that will shape the future of the industry.

The use of artificial intelligence (AI) and automated speech recognition (ASR) technologies in the creation of court transcripts presents serious concerns. Legal professionals, including attorneys, have also begun using notetaker apps in sensitive legal environments, often without the knowledge or consent of all parties involved. These technologies pose significant threats to the security, confidentiality, integrity, and verifiability of the legal process.

This briefing examines some of these risks, focusing intentionally more narrowly on 1) the security risks associated with deploying transcription and notetaker apps in legal proceedings such as depositions and in courtrooms, 2) privacy concerns and the potential for misuse of or unauthorized access to sensitive information, 3) model drift, technical limitations and hallucination risks, 4) provenance and custody concerns, and 5) ethical and confidentiality challenges. It also highlights how the unauthorized or undisclosed use of AI/ASR tools and notetaker applications can undercut the administration of justice and diminish public trust in our legal system.

What are AI Transcription Tools and Notetaking Apps?

AI transcription tools and notetaking apps utilize automatic speech recognition and natural language processing to convert speech to text, create automated summaries, generate searchable records, and translate foreign languages, among other things. There are various AI notetaking apps which are designed to join or listen to depositions or meetings and generate notes. However, utilizing these apps may put users on the wrong side of the federal or state court rules for depositions (see FRCP 30), ABA client-confidentiality, technology competence, and vendor-oversight duties, as well as in violation of multiple state consent/wiretap laws. While AI systems predict statistically likely language, they do not verify what was actually said. Frequently gaps are filled when audio is unclear. In addition, the myth of “human review” protocols touted in marketing language is flawed, because human reviewers are relying on what could be inaccurate or flawed ASR transcription when they were not present to witness, understand, or know what may be inaccurate. Consequently, attorneys, courts, and litigants inherit downstream risks.

Security Risks Associated with Notetaking Apps in Legal Settings

1. Data Breaches and Unauthorized Access – Legal proceedings frequently involve highly sensitive data, including personal information, confidential business details, trade secrets, privileged communications, and sensitive national security information when involving transcription vendors who may have government contracts and are utilizing speech recognition in their processing. “Tools like Otter.ai, Fireflies.ai, and Microsoft Copilot promise to enhance efficiency, but their use raises significant concerns regarding privacy, data security, and regulatory compliance.”¹ One significant reason for concern is these tools typically process audio streams that are stored in the cloud and include third-party vendors. “Unlike informal handwritten notes, these records can be subject to legal discovery, regulatory disclosure requests, and privacy claims if not governed properly.”²

Many AI notetaker apps can be difficult to detect when integrated through meeting platforms. Research has shown that certain videoconferencing applications may retain microphone access and transmit audio-derived telemetry even when users believe they are muted. Kassem Fawaz, an assistant professor of electrical and computer engineering at the University of Wisconsin- Madison, investigated this issue. “It turns out, in the vast majority of cases, when you mute yourself, these apps do not give up access to the microphone,” says Fawaz. “And that’s a problem. When you’re muted, people don’t expect these apps to collect data.”³ This does not establish covert recording by AI notetaking applications, but it demonstrates that users should not assume muting alone prevents audio access.

2. Automated Data Extraction – Although many enterprise and business tiers contractually exclude customer data from training, it is incumbent on the users of these systems to recognize the dangers of exposing confidential content. AI/ASR systems excel at parsing and categorizing large volumes of speech data, but this capability may also be misused. When these systems process court transcripts, depositions, or legal discussions captured through notetaker apps, sensitive information may be scraped, aggregated, reused for model training, or disclosed to unauthorized third parties. “If an AI system makes an error, determining responsibility is not straightforward.”⁴ Compounding the problem, meeting participants may not review or correct AI-generated notes. “As a result, errors may become part of ‘the record.’”⁵

3. **Lack of Chain of Custody** – Traditional legal transcripts rely on identifiable custodianship and strict authentication, such as sworn certifications of accuracy, notary seals, and unbroken digital or physical chains of custody. These requirements guarantee that a transcript is a true and accurate record of the original proceeding, satisfying evidentiary foundations like [Federal Rules of Evidence 901](#) and [902](#). Notetaker applications may permit recordings or transcript text to be exported, modified, or redistributed without reliable tracking mechanisms. For that and other reasons, before adopting notetaking apps, companies should establish clear internal protocols on their appropriate use, conduct security and contractual vetting of all associated upstream and downstream vendors, review data transfer mechanisms, and obtain required disclosures or consent in privileged or highly sensitive settings.

4. **Inadvertent Waiver of Privilege** – Precedents from courts establish that sharing privileged or confidential information with third-party AI platforms, including public AI notetakers, can breach confidentiality and trigger an irreversible waiver of attorney-client privilege. In a novel decision under [United States v. Heppner](#), Judge Rakoff of the Southern District of New York held that “certain written exchanges that defendant (...) had with a generative artificial intelligence (‘AI’) platform were not protected from Government inspection by either the attorney-client privilege or the work product doctrine.”⁶ As one outside practitioner notes in the wake of this decision, “clients should assume that anything entered into a public AI tool may be discoverable.”⁷

5. **Failure to Obtain Consent** – Some legal participants may use AI notetaker applications without disclosing the recording or processing of conversations to all parties involved. If the intent is to route client communications through an AI vendor, the [American Bar Association’s Solo, Small Firm and General Practice Division recommends](#) that attorneys should transparently disclose AI use during privileged communications, explaining potential risks, and obtain explicit informed consent. It goes on to warn that many states have wiretapping laws requiring consent from all parties to record the conversations. Although no case law yet addresses AI notetaking directly, existing precedents applying privilege waiver to third-party platforms make clear the stakes.⁸

Privacy Concerns

1. **Privacy Concerns** – The use of AI/ASR systems and notetaker applications raise substantial privacy concerns specifically because there are no uniform standards governing the handling, storage, retention, or downstream use of sensitive legal data. Any proposed AI solution must comply with all existing privacy regulations and standards to ensure anonymity, confidentiality, and control, including wiretapping laws across the country. In addition to data breaches, “digital” solutions in court reporting are often reliant on either outsourcing (gig workers, even overseas entities) or large language models (LLMs). The overseas gig workers are unregulated, while LLMs are vulnerable to data scraping; both are potential vulnerabilities for data loss. End-user agreements are quick to award themselves all the benefits of data access with none of the liability. The ABA has been clear in its [Formal Opinion 512](#): Lawyers are responsible for loss of data even through a third-party vendor that exposes a client’s personal or proprietary data -- HIPAA, PII, or intellectual property, to name a few.⁹

2. **Unintended Data Exposure** – Witness safety is paramount in legal proceedings. AI/ASR systems and notetaker apps may capture and store addresses, phone numbers, personal

identifying information, and/or protected testimony, creating substantial risks if that data is breached or shared without authorization. In its [Formal Opinion 2025-6](#), the New York City Bar Association advises, “If an attorney knows that a client is recording a call with an AI tool, the lawyer should advise the client of the disadvantages of doing so.”¹⁰

3. **Encryption** – IBM explains, “Encryption works by using encryption algorithms to scramble data into an indecipherable format. Only the authorized parties with the right secret key, known as a decryption key, can unscramble the data.”¹¹ It is universally applied to three core states—**at rest** (stored), **in transit** (moving across networks), and **in use** (being processed in memory)—across both on-premises setups and cloud environments. While data is easily secured *at rest* and *in transit* using standard methods, protecting data *in use* requires advanced cryptographic or hardware-based architectures that are resource-intensive and remain absent from mainstream commercial transcription pipelines. [RAND further clarifies](#), “Such (*in use*) protection is often achieved through hardware-based attested trusted execution environments (TEEs). A TEE is an isolated environment within a computer system that prioritizes security and confidentiality when executing sensitive computations. Using a memory encryption engine, TEEs encrypt data before they are stored in memory and decrypt the data only when computation is required.”¹²

Model Drift, Technical Limitations, Biases, and Hallucination Risks

1. **Model Drift and degrading data** – AI/ASR systems continue to struggle with legal terminology, overlapping dialogue, emotional speech, diverse accents, and rapidly changing courtroom dynamics. These systems often face performance degradation in real-world environments, particularly under domain shift, data scarcity, and complex acoustic conditions. “Background noise in real environments (such as traffic, crowd noise, device fans) mixes with the target speech signal, reducing the signal-to-noise ratio and masking critical acoustic features.”¹³ It’s ubiquitous. Further, “Noise not only reduces the clarity of the speech signal but also introduces acoustic features an LLM model has not learned, leading to a sharp increase in recognition error rates. The reverberation effect, i.e., speech distortion caused by sound wave reflections in enclosed spaces, also severely affects ASR performance. The impact of reverberation and noise on ASR performance is well-known.”

While ASR has seen improvements over the years, it is of significance that one of the industry’s leading ASR providers acknowledges that the technology has not yet reached professional-grade reliability. In its 2025 [State of ASR Report](#), 3Play Media reports that “[O]ne clear trend in this year’s data: the pace of improvement is beginning to level off. While previous years brought more dramatic gains in accuracy, recent advances have felt more incremental.”¹⁴ The company further recommends human review—not ASR alone—for disability accommodation despite promoting its own proprietary ASR engine.

Unlike stenographic methods, many ASR systems continuously evolve through updates that are not transparent to courts or litigants. There is often no reliable audit trail documenting the precise model version, training data, or post-processing layers used to generate a transcript. “Adding to the complexity, many organizations are deploying these tools because they are marketed as cost-saving alternatives to human note taking; however, while automation can reduce up-front administrative expense, the downstream costs of inconsistent records, misattribution or privilege loss can far exceed any upfront efficiencies.”¹⁵

2. Technical Limitations – Courtrooms and remote meeting rooms are rarely acoustically optimized environments. Multi-speaker ASR is different from single-speaker ASR in that its purpose is to transcribe speech from an audio containing multiple speakers whose speech may overlap. In contrast to single-speaker ASR, which focuses on *what was said* by one speaker, multi-speaker ASR additionally determines who actually said what. Unfortunately, a [focused study](#) concluded that “monaural multiple speaker ASR remains challenging due to data scarcity (in LLMs) and the intrinsic difficulty of recognizing and attributing words to individual speakers, particularly in overlapping speech.”¹⁶

AI/ASR systems are particularly vulnerable when speakers are under stress or exhibiting disfluencies such as pauses, stutters, fragmented speech, false starts, or incomplete phrases. In the legal setting, these moments often contain legally significant testimony that may be omitted or normalized by ASR systems.

3. Biases, Hallucination Risks, and Fabricated Content – Modern AI/ASR systems may generate hallucinated content: fabricated or altered words, phrases, or sentences that were never spoken in the original proceeding. The [National Center for State Courts warns](#), “LLM’s predictive nature generates text that *sounds right* rather than text that *is right*. This creates hallucinations that can be dangerously convincing.”¹⁷

In legal settings, hallucinations are not mere transcription errors, they are fabricated content capable of materially altering testimony, judicial rulings, admissions, or the appellate record itself. “LLMs are essentially a predictive text function — like the recommended next words that appear when typing a text message, but on a far larger scale. They generate text that they predict is desired.”¹⁸

According to Cornell researchers, when someone speaks a little too haltingly and/or with long pauses, an automatic speech-to-text transcription tool might put harmful, incendiary words in the speaker’s mouth. “With hallucinations, artificial intelligence is making up something from nothing,” said Allison Koenecke, assistant professor of information science in the Cornell Ann S. Bowers College of Computing and Information Science. “That can lead to huge downstream consequences if these transcriptions are used in the context of AI-based hiring, in courtroom trials or patient notes in medical settings.”¹⁹

A 2024 study by Koenecke, Choi, Mei, Schellmann, and Sloane, [Careless Whisper: Speech-to-Text Hallucination Harms](#) specifically focused on fabricated-content claims. The study found that “While many of Whisper’s transcriptions were highly accurate, we find that roughly 1% of audio transcriptions contained entire hallucinated phrases or sentences which did not exist in any form in the underlying audio. We thematically analyze the Whisper-hallucinated content, finding that 38% of hallucinations include explicit harms such as perpetuating violence, making up inaccurate associations, or implying false authority.” The study also found that “hallucinations disproportionately occur for individuals who speak with longer shares of non-vocal durations—a common symptom of aphasia.”²⁰ In courtroom settings, the aphasia finding matters: the speakers most likely to invoke aphasic hallucinations are elderly, disabled, or witnesses offering emotionally charged testimony, exactly the testimony court transcripts need to get right.

An [Associated Press investigation](#) of Whisper in medical transcription, also in 2024, documented hallucinated content in deployed clinical tools and reported that at least one vendor deletes the original audio after transcription, destroying the only means of

verification. That's a real-world illustration of the importance of chain of custody: if the audio is gone, the fabrication is undetectable and the record is unimpeachable in the worst sense. In other words, "You can't catch errors if you take away the ground truth," said William Saunders, a former OpenAI engineer.²¹ Even in a favorable study of ASR, [*Robust Speech Recognition via Large-Scale Weak Supervision*](#), Radford et al. acknowledge hallucination and repetition as failure modes.²²

Researchers have documented hallucinations in commercial ASR systems, including fabricated statements, invented racial commentary, and entirely nonexistent dialogue appearing in transcripts generated from degraded or silent audio. A [*subsequent study*](#) concluded, "While similar to conventional decoding errors in potentially compromising the usability of transcriptions for downstream applications, hallucinations can be more detrimental due to their preservation of syntactically and semantically plausible structure. This apparent coherence can mislead subsequent processing stages and introduce serious risks, particularly in critical domains such as healthcare and law."²³

In their landmark study, [*Racial Disparities in Automated Speech Recognition*](#), Koencke et al. found that five commercial ASR systems showed roughly double the word error rate for Black speakers relative to white speakers (approximately 0.35 versus 0.19 average WER). "Despite variation in transcription quality across systems, the error rates for Black speakers are nearly twice as large in every case."²⁴ These findings are corroborated in a [*more recent study*](#) across leading ASR platforms.²⁵ The disparity exists because acoustic models and natural language processing systems historically rely on training datasets that overrepresent standard American English and underrepresent Black speakers and dialects like African American English (AAE). According to University of Chicago Asst. Prof. Sharese King, the clearest distinctions between AAE and standardized American English often revolve around grammatical differences in vocabulary, accents, and how speakers use verb aspects or tenses to describe how an event unfolded. "If we continue to ignore the field of AI as a space where racism can emerge, then we'll continue to perpetuate the stereotypes and the harms against African Americans," says King.²⁶

Unlike stenographic errors, which are attributable to identifiable human professionals and verifiable notes, hallucinated ASR content has no identifiable human author. This creates profound concerns regarding accountability, authentication, evidentiary reliability, and due process. Also noteworthy: In the [*largest study*](#) of English human and ASR broadcast captions in three countries (the U.S., U.K. and Canada) over four years (2018 to 2022), which included approximately 17,000 live captions, "human caption accuracy was significantly higher, achieving 98.9% to 99.4% accuracy compared to ASR's 95.7% to 96.3%."²⁷

Provenance, Authentication, and Due Process Concerns

1. Provenance, Authentication, and Due Process Concerns – Many ASR-generated transcripts lack sufficient provenance to permit meaningful forensic validation or authentication. Courts and litigants may have no access to the underlying model, version history, confidence scoring, training datasets, editing history, or automated cleanup layers used to create the final transcript. "From a practical standpoint, poor traceability makes it hard to align AI training datasets with intended use cases, which could result in lower-quality models."²⁸ Without this information, parties may be unable to challenge transcript reliability or reconstruct how the official record was produced.

2. *Ownership and Accountability* –A team of multidisciplinary researchers, including Professor Sandy Pentland and others from MIT, created the [Data Provenance Initiative](#)²⁹ to tackle the data transparency challenge head-on. However, no solution yet exists that solves the issue of ownership or accountability without the critical Human-in-the-Loop (HITL), even for matters classified as “moderate risk” much less the “high risk” setting of a court of law. The responsibility and ultimately the liability for the creation and transmittal of court records must always be tied back to a named individual who is answerable for decisions made along the way. When liability can be traced to a specific person, such as a certified or official court reporter, it prevents negligence, protects against unauthorized alteration, and preserves the integrity of the judicial process.

3. *Courts Should Endorse Technical Safeguards* – Federal Rule of Evidence 902(13) and 902(14) recognize self-authentication of electronic evidence through hash verification and certification. Digital recording systems used in legal proceedings should, at a minimum, hash-seal recordings at capture, preserve the original multi-channel audio, log the model and software version used for each transcription pass, maintain immutable audit trails, and retain original audio for independent verification. Emerging provenance standards such as C2PA provide additional mechanisms for documenting authenticity.³⁰ At present, no widely accepted certification regime evaluates legal-domain ASR systems for transcription accuracy, speaker attribution, hallucination rate, provenance, and accountability under courtroom conditions.

4. *Human Review of Transcripts in Legal Proceedings* – Many commercial transcription vendors advertise a human-in-the-loop (HITL) review process in which a person reviews machine-generated output before it is delivered to the customer; however, a human cannot meaningfully review what they cannot understand. When the audio quality drops below a human's ability to discern what is being said, human review of an ASR generated transcript becomes impossible. This highlights a major reliance: ASR validation fundamentally depends on a human reviewer being able to cross-reference the text with understandable, intelligible audio.

Researchers at Vanderbilt Law School and the University of Colorado have formalized the spectrum of human involvement in AI systems into three specific categories: 1) Human-in-the-loop (HITL) requires human approval before any AI output becomes actionable; 2) Human-on-the-loop (HOTL) allows the AI to act autonomously while a human monitors and can intervene; and 3) Human-out-of-the-loop (HOOTL) removes the human from the output entirely. “For legal work involving privileged information, client-facing communications, or binding obligations, only HITL meets the professional standard. The legal profession's fiduciary obligations, confidentiality requirements, and professional responsibility rules make human oversight not a best practice but a non-negotiable structural requirement.”³¹

5. *Make sure your HITL is qualified* – While human review can improve readability and correct errors, the quality and reliability of that review depend upon the reviewer's qualifications, specialized training, access to the original audio, as well as familiarity with legal terminology and legal proceedings. Of equal import, the reviewer must be individually accountable for the accuracy of the work product.

6. *Speaker Attribution (Diarization)*

Transcription accuracy is only part of the reliability question. Speaker attribution—correctly identifying who said what—is equally important because attributing an admission or statement to the wrong speaker can materially alter the legal record. Peer-reviewed research shows diarization performance degrades as overlapping speech, interruptions, and conversational complexity increase, conditions commonly encountered during legal proceedings. Lockton VPs Anthony and Noon warn, “Notetaking tools may misidentify speakers, especially in multi-party meetings, leading to erroneous attributions.”³²

Ethical and Confidentiality Challenges

1. *Guidance in the Legal Community* – When it comes to ethics, national and local leaders are currently grappling with and authoring the first generation of guidance for the legal community. In a trailblazing publication in December 2025, the New York City Bar Association’s Committee on Professional Ethics issued [Formal Opinion 2025-6: *Ethical Issues Affecting Use of AI to Record, Transcribe, and Summarize Conversations with Clients*](#).³³ While the opinion is not binding outside of NY, it offers a foundation for common scenarios of AI capturing conversations with clients.

2. *Compliance with Legal Standards* – Attorneys, judges, and court reporters have an obligation to strictly adhere to professional codes, confidentiality standards, evidentiary rules, and applicable professional conduct requirements, including [ABA Formal Opinion 512](#) and related supervisory obligations under [Model Rule 5.3](#). In states with mandatory court reporter certification laws, it is the responsibility of all court reporters to follow the laws and rules within the states where they practice. For officials working directly with the courts, they are officers of the court, and they must follow all procedural policies, codes, and court rules. The National Court Reporters Association (NCRA) has issued a [formal statement regarding the use of AI](#).³⁴ NCRA also has a [Code of Professional Ethics – Guidelines for Professional Practice](#) that affiliated court reporters are required to adhere to and follow. By contrast, AI tools are accountable to none of the same legal, ethical, and professional standards.

3. *Recent litigation, regulatory developments, catastrophic court transcription failure*
Recent litigation reinforces that AI meeting assistants, notetaker applications, and AI-generated transcripts are receiving judicial and regulatory scrutiny. The following matters are discussed as pending developments rather than adjudicated findings:

[Black v. City of San Diego](#), No. 21-cv-01990-RBM-JLB, slip op. at 6–8 (S.D. Cal. May 2, 2025). The Court denied Plaintiff request to conduct depositions by video and to prepare transcripts using AI/ASR, citing accuracy, competency, and data privacy concerns.

[Snyder v. Lindblad Expeditions LLC](#), No. 2:25-cv-01753-LK, slip op. at 5–6 (W.D. Wash. Jan. 20, 2026). The Court denied Plaintiff’s motion to conduct remote depositions audio/video recording without a court reporter to be transcribed after the fact, specifically stating that Plaintiff failed to prove “that the resulting recordings would have sufficient indicia of reliability to be used as the ‘official record.’”

[Juno v. Amare](#), No. CV-2008-901100 (Cir. Ct. Baldwin Cnty., Ala. Dec. 13, 2012). A jury awarded \$140 Million Verdict for Wrongful Death of a Patient Due to Medical Transcription

Errors. Thomas Hospital was held accountable for the incorrect transcription written down by its outsourced medical transcription company and that the error survived into the final medical record.

[*Mata v. Avianca, Inc.*](#), 678 F. Supp. 3d 443 (S.D.N.Y. 2023). While involving fabricated legal citations rather than transcription, illustrates the broader principle that fluent AI output can appear authoritative while containing material errors, reinforcing the need for independent verification.

The following matters are discussed as pending developments rather than adjudicated findings:

[*In re Otter.AI Privacy Litigation*](#), No. 5:25-cv-06911-EKL (N.D. Cal. filed Aug. 15, 2025), originally filed as *Brewer v. Otter.ai* and later consolidated, alleges violations of the federal Electronic Communications Privacy Act (ECPA) where Otter unlawfully intercepted and recorded private communications in real time. (The litigation remains pending as of this publication but crucially, its ECPA claims have survived a defendant's motion to dismiss.)

[*Eto v. Mayo Clinic*](#), No. 0:26-cv-03189 (D. Minn. July 6, 2026) a former research operations director at the Mayo Clinic says the healthcare institution demoted and later fired her for reporting its deviation from federal requirements for clinical research on human subjects. Ten separate whistleblower reports raised similar concerns, including allegations that study investigators were trying to disguise a 67 percent error rate.

[*Chamberlain v. Granola, Inc.*](#), No. 3:26-cv-07926 (N.D. Cal. July 30, 2026). (No. 3:26-cv-07926) is a proposed class action filed on July 30, 2026, in the U.S. District Court for the Northern District of California. The lawsuit accuses the AI meeting notetaker Granola of recording private conversations without all-party consent and feeding those transcripts into AI model training by default. Unlike competing tools that send a visible bot into a Zoom or Microsoft Teams call, Granola records audio locally from the user's microphone device without appearing as a participant. The lawsuit claims Granola markets this hidden nature as a feature ("Other people in the room won't know it's there").

Australia's primary court transcription provider allegedly recently entered voluntary administration following an [ABC News](#) investigation that revealed unauthorized, offshore handling of sensitive court data Greens Senator David Shoebridge, who sits on the legal and constitutional affairs committee, said the federal courts' reputation had been damaged. "This kind of essential public service should never have been [privatized] in the first place, and now that the monopoly corporate provider is exiting, it leaves the court system in a shambles," he said. "Whoever signed and oversaw this contract needs to front Senate Estimates and explain what due diligence they did on a company that has offshored private information, now gone broke and seriously damaged the reputation of our Federal Courts."³⁵

The [EU AI Act](#) is the world's first comprehensive legal framework for artificial intelligence, regulating developers and deployers based on risk. It prohibits unacceptable AI practices, classifies AI intended for use in the administration of justice as high-risk, and emphasizes logging, transparency, and human oversight.³⁶ Domestically, the [NIST AI Risk Management Framework](#)³⁷ and [ISO/IEC 42001](#)³⁸ provide technology-neutral governance frameworks consistent with the recommendations in this briefing.

Conclusion

The widespread adoption of AI/ASR technologies and notetaker applications for the creation of legal transcripts or even internal documents introduces substantial vulnerabilities and risks. These include data breaches, unauthorized data scraping, manipulation of legal proceedings, privacy violations, hallucinated content, provenance failures, lack of accountability, and potential waiver of attorney-client privilege.

Courts and legal stakeholders must recognize that modern AI/ASR systems introduce risks beyond ordinary transcription error, including model degradation, domain drift, and fabricated content generated without a transparent audit trail or identifiable human author. These risks create unique evidentiary, constitutional, and due process concerns fundamentally different from traditional human transcription methods. Courts and legal stakeholders must be able to rely on system performance with consistently accurate and valid outputs. Failures in court have real-world consequences.

Artificial intelligence will continue to evolve, and its capabilities should be evaluated through independent, transparent testing rather than predictions about future performance. The Coalition's position is not that AI should be excluded from legal proceedings, but that technology used to create or certify the official legal record should satisfy objective, published acceptance criteria.

Before AI-generated transcripts are relied upon as the official legal record, the technology should demonstrate independently validated performance on representative legal-domain audio, including published thresholds for word accuracy, speaker attribution, and hallucination rates. Systems should also provide documented provenance, model version logging, immutable retention of original audio, and auditable processing histories sufficient to support independent verification.

In addition, because a notetaker app creates a second, unsanctioned recording of proceedings that is outside the officer's control, it risks unauthorized disclosure of privileged information to a third-party vendor, it may violate wiretapping laws, and can therefore breach ABA duties (Rules 1.6, 1.1cmt. [8], 5.3, 1.4)³⁹ and violate FRCP 30(b)(3) and FRCP 80⁴⁰, which states: "If stenographically reported testimony at a hearing or trial is admissible in evidence at a later trial, the testimony may be proved by a transcript certified by the person who reported it." They may also breach confidentiality requirements for attorneys and court reporters across the country.

Certified court reporters are not only tested to accuracy, speed, and knowledge-based standards, they have mandatory continuing education requirements, they are governed by codes of ethics and are individually held accountable for their work product.

AI/ASR transcription alone and/or with an unqualified human in the loop should not assume the role currently assigned to a certified court reporter unless a comparable certification, accountability, and oversight framework exists for AI systems. Establishing objective standards for performance, transparency, authentication, and accountability provides policymakers with a technology-neutral framework that encourages innovation while preserving the integrity of the official legal record.

Recommended Policy Implementations

To safeguard the integrity of the legal system and preserve public confidence, governmental policymakers, courts, attorneys, court reporters, and legal professionals should:

1. Establish clear regulations and policies governing the use of AI/ASR systems and note-taker applications in legal settings, including: use the officially noticed method of recording only; obtain proper consent from all participants; and ensure proper safeguards are in place before deploying AI notetaking apps. FRCP 30(b)(3) and most state court rules require the noticing party to state the recording method in the notice; any additional recording method requires prior notice to the deponent and other parties;
2. Require transparency, disclosure, and consent regarding the use of AI/ASR technologies in transcript creation or summarization. If the officer before whom the deposition is being taken or the moderator of a virtual courtroom notices an uninvited notetaking bot has joined the meeting, they should ask the meeting host to stop recording or simply remove the bot like they would any uninvited guest. The record must be made by and/or under the direction of the officer. Advise all participants that private notetaker bots/apps are outside the officer's control;
3. Mandate strong encryption, access controls, and independent security audits for systems managing legal proceedings, as well as develop authentication and provenance standards for digitally created transcripts;
4. Ensure that parties retain the ability to challenge and verify transcript reliability when produced by AI apps through identifiable and auditable methods; In December 2025, the ABA Task Force on Law and Artificial Intelligence published a [report](#) that included general, non-technical guidelines for how judicial officers can responsibly use AI. The National Center for State Courts also issued [guidance](#) for the use of AI in the courts and maintains an interactive [state map](#) of updated guidance based on court orders, rules, and proposed policies;⁴¹
5. Preserve meaningful human accountability in the creation and certification of legal records; and,
6. Because AI creates a growing category of uninsured risks, enterprises should explore explicit protection for AI-driven liability.

By proactively addressing these concerns, the legal community can help ensure that technology serves as an aid to justice rather than a threat to the integrity of the judicial record.

About Jeopardizing Justice

Jeopardizing Justice is a coalition of court reporting experts dedicated to protecting the integrity of legal proceedings and records upon which citizens rely for the fair administration of justice. For more information, visit www.jeopardizingjustice.com.

The primary authors are of this briefing, Phyllis Craver Lykken, FAPR, RPR, CCR CSR, NCRA Past Director; Sue A. Terry, FAPR, RPR, CRR, CRC, NCRA Past President; Sierra Zanghi, B.A., RSR, CCR; Debra Dibble, FAPR, RDR, CRR, CRC, NCRA Past President; Kristin Anderson, M.A., RPR, CRI, FCRR, CSR, NCRA Past President; and contributing editors, Liz A. Harvey, FAPR, RPR, CCR, CSR; Mary Pierce, CSR; Lisa Migliore Black, CCR; Stefanie Allison, RPR, CSR, and Doug Bettis, OCR, are court reporters concerned about maintaining a secure justice system. They are members of a profession with an economic interest in the use of transcription technologies in legal proceedings.

Independent Endorsing Reviewers:

Moez Ben-Azzouz, *Professor of Mathematics at Sinclair College in Dayton, Ohio, and Director of Cybersecurity Studies and Certification at Wittenberg University in Springfield, Ohio.* Mr. Ben-Azzouz brings more than 24 years of teaching and training experience across mathematics, cybersecurity, computer science, and machine learning and AI. He holds more than 30 industry certifications in these fields, including credentials in SecAI, the emerging discipline at the intersection of cybersecurity and artificial intelligence.

“As someone who builds AI models, understands and teaches the technology, I am not an abolitionist when it comes to AI but I am against the mindless and relentless way it is being unleashed on us without any pause, thought, or discussions of the damage being done.”

Edward Primeau, *Primeau Forensics.* Mr. Primeau attended the University of Detroit. He founded Primeau Forensics in 1984, a digital media forensics laboratory specializing in the authentication, enhancement, recovery, and transcription of audio, video, and image evidence for legal and investigative use. The company is based in Rochester Hills, Michigan, and has operated for nearly 40 years. Primeau Forensics processes more than 250 cases annually and has completed over 5,000 forensic investigations to date, with expert testimony delivered in more than 500 local, state, federal, and international court cases. “As an audio/video forensic expert with more than four decades of experience, I found this paper to be a thoughtful, well-researched, and persuasive examination of the risks associated with AI transcription tools and notetaking applications in legal proceedings. It clearly identifies significant concerns involving authentication, provenance, chain of custody, privacy, reliability, and the integrity of the official record.”

National Court Reporters Association (NCRA) is recognized worldwide as the leading authority on capturing and transcribing the spoken word into writing. The organization’s mission is to apply the knowledge and experience of verbatim stenographic reporters working in cooperation with the courts and bars toward improving the criminal and civil justice system to best serve the public good.

Legal disclaimer: Jeopardizing Justice (JJ) is committed to providing accurate and up-to-date information in our seminars and presentations. The content is not offered as legal advice. While JJ endeavors to keep the information updated and correct, JJ does not make representations or warranties of any kind, express or implied, about the completeness, accuracy, or reliability of the information provided. You should always seek the advice of a licensed attorney for any legal questions. In no event shall JJ, its employees, or contractors be liable to you for any claims, penalties, losses, damages, or expenses, howsoever arising, including, and without limitation, direct or indirect loss, or consequential loss, in connection with the use of the information within this briefing. It is your responsibility to know the appropriate laws and court rules governing your state.

Resources - This bibliography highlights principal authorities supporting this briefing. Readers are encouraged to consult the original sources and verify current versions for authority.

-
- ¹ Josephine Law, *AI Notetakers in Meetings: Balancing Efficiency with Privacy and Risk*, PRIVACY AT FORDHAM UNIV. (Feb. 19, 2025), <https://privacy.blog.fordham.edu/ai-notetakers-in-meetings-balancing-efficiency-with-privacy-and-risk> [<https://perma.cc/5VV4-NMRA>].
- ² Kaitlin Betancourt et al., *AI Transcription Tools Under Scrutiny: Navigating Privacy Risks and Practical Mitigation Strategies*, JD SUPRA (Apr. 29, 2026), <https://www.jdsupra.com/legalnews/ai-transcription-tools-under-scrutiny-2028942> [<https://perma.cc/M5Y4-5F6T>].
- ³ Jason Daley, *You're Muted — Or Are You? Videoconferencing Apps May Listen Even When Mic Is Off*, UW-MADISON NEWS (Apr. 11, 2022), <https://news.wisc.edu/youre-muted-or-are-you-videoconferencing-apps-may-listen-even-when-mic-is-off> [<https://perma.cc/X9K9-8PBA>].
- ⁴ *How Is AI Impacting the Legal Profession?*, VANDERBILT L. SCH. (Jan. 20, 2026), <https://law.vanderbilt.edu/master-legal-studies/articles/how-is-ai-impacting-the-legal-profession> [<https://perma.cc/MU8M-PLN9>].
- ⁵ Nicola Anthony & James Noon, *AI Notetaking and Transcription: Risk Management Considerations and Best Practices*, LOCKTON (Oct. 24, 2025), <https://global.lockton.com/gb/en/news-insights/ai-notetaking-and-transcription-risk-management-considerations-and-best> [<https://perma.cc/MK5L-JQ7X>].
- ⁶ *United States v. Heppner*, 820 F. Supp. 3d 292 (S.D.N.Y. 2026), <https://storage.courtlistener.com/recap/gov.uscourts.nysd.652138/gov.uscourts.nysd.652138.27.0.pdf>.
- ⁷ Mark G. McCreary, *Federal Court Holds AI Chats Are Not Privileged*, FOX ROTHSCHILD (Feb. 18, 2026), <https://www.foxrothschild.com/publications/federal-court-holds-ai-chats-are-not-privileged> (PDF on file with author).
- ⁸ Gabriel Buehler, *AI and You: Confidentiality Risks of Using Transcription and Note-Taking Software During Meetings*, GPSOLO EREPORT (Aug. 27, 2025), <https://www.americanbar.org/groups/gpsolo/resources/ereport/2025-september/ai-you-confidentiality-risks-meeting-transcription-note-taking-software> [<https://web.archive.org/web/20250907052035/https://www.americanbar.org/groups/gpsolo/resources/ereport/2025-september/ai-you-confidentiality-risks-meeting-transcription-note-taking-software>].
- ⁹ ABA Comm. on Ethics & Pro. Resp., Formal Op. 512 (2024), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf [<https://perma.cc/SKV9-GWAX>].
- ¹⁰ N.Y.C. Bar Ass'n Comm. on Pro. Ethics, Formal Op. 2025-6 (2025), <https://www.nycbar.org/reports/formal-opinion-2025-6-ethical-issues-affecting-use-of-ai-to-record-transcribe-and-summarize-conversations-with-clients> [<https://perma.cc/A894-N8PY>].
- ¹¹ *What Is Encryption?*, IBM, <https://www.ibm.com/think/topics/encryption> [<https://perma.cc/ZR25-CLL6>] (last visited Aug. 19, 2026).
- ¹² Quentin E. Hodgson et al., *AI Security Guide and Risk Assessment Tool; Appendix A, Confidential Computing, Secure Enclaves, and Attestation*, RAND CORP. (Feb. 12, 2026), <https://doi.org/10.7249/TLA4174-1>.
- ¹³ Hua Zhong, Fang Qin & Chunzhi Wu, *Research Status on Performance Degradation of Automatic Speech Recognition Models*, in PROCEEDINGS OF THE 2025 8TH INTERNATIONAL CONFERENCE ON COMPUTER INFORMATION SCIENCE AND ARTIFICIAL INTELLIGENCE 1209, 1209–14 (2025), <https://doi.org/10.1145/3773365.3773556>.
- ¹⁴ 2025 STATE OF AUTOMATIC SPEECH RECOGNITION (3Play Media 2025), <https://go.3playmedia.com/rs-2025-asr> (PDF on file with author).
- ¹⁵ Joel M. Cohen & Mark Davies, *When Every Word Is Recorded: AI Meeting Tools and the New Governance Risks*, WHITE & CASE (Nov. 3, 2025), <https://www.whitecase.com/insight-alert/when-every-word-recorded-ai-meeting-tools-and-new-governance-risks> [<https://perma.cc/X5AG-E8WH>].
- ¹⁶ Xinlu He & Jacob Whitehill, *Survey of End-to-End Multi-Speaker Automatic Speech Recognition for Monaural Audio*, arXiv:2505.10975 (rev. May 27, 2026), <https://arxiv.org/abs/2505.10975> [<https://perma.cc/CTM7-7YRP>].
- ¹⁷ TRI/NCSC AI Policy Consortium for Law & Courts, *A Legal Practitioner's Guide to AI & Hallucinations*, NAT'L CTR. FOR STATE CTS. (Feb. 16, 2026), <https://www.ncsc.org/resources-courts/legal-practitioners-guide-ai-hallucinations> [<https://perma.cc/EV9K-TSBZ>].
- ¹⁸ Ibid. See TRI/NCSC AI Policy Consortium for Law & Courts.

-
- ¹⁹ Louis DiPietro, *AI Speech-to-Text Can Hallucinate Violent Language*, CORNELL CHRON. (June 11, 2024), <https://news.cornell.edu/stories/2024/06/ai-speech-text-can-hallucinate-violent-language> [<https://perma.cc/WEG9-D7QS>].
- ²⁰ Allison Koenecke et al., *Careless Whisper: Speech-to-Text Hallucination Harms*, in PROCEEDINGS OF THE 2024 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 1672, 1672–81 (2024), <https://doi.org/10.1145/3630106.3658996>.
- ²¹ Garance Burke & Hilke Schellmann, *Researchers Say AI Transcription Tool Used in Hospitals Invents Things No One Ever Said*, ASSOCIATED PRESS (Oct. 26, 2024), <https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14> [<https://perma.cc/39WP-P47Y>].
- ²² Alec Radford et al., *Robust Speech Recognition via Large-Scale Weak Supervision*, 202 PROC. MACH. LEARNING RSCH. 28492, 28492–28518 (2023), <https://proceedings.mlr.press/v202/radford23a.html> [<https://perma.cc/R3WH-4X87>].
- ²³ Alkis Koudounas et al., *Hallucination Benchmark for Speech Foundation Models*, arXiv:2510.16567 (Oct. 18, 2025), <https://arxiv.org/abs/2510.16567> [<https://perma.cc/RCH5-Y45R>].
- ²⁴ Allison Koenecke et al., *Racial Disparities in Automated Speech Recognition*, 117 PROC. NAT’L ACAD. SCIS. U.S.A. 7684, 7684–89 (2020), <https://pubmed.ncbi.nlm.nih.gov/32205437>.
- ²⁵ Maliha Jahan et al., *Unveiling Performance Bias in ASR Systems: A Study on Gender, Age, Accent, and More*, in 2025 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING (ICASSP) 1, 1–5 (2025), <https://doi.org/10.1109/ICASSP49660.2025.10887767>.
- ²⁶ Tori Lee, *AI Is Biased Against Speakers of African American English, Study Finds*, U. CHI. NEWS (Sept. 17, 2024), <https://news.uchicago.edu/story/ai-biased-against-speakers-african-american-english-study-finds> [<https://perma.cc/HDU5-3BGR>].
- ²⁷ Pablo Romero-Fresco & Nazaret Fresno, *The Accuracy of Automatic and Human Live Captions in English*, 22 LINGUISTICA ANTVERPIENSIA, NEW SERIES: THEMES IN TRANSLATION STUDIES 114, 114–33 (2023), <https://doi.org/10.52034/lans-tts.v22i.774>.
- ²⁸ Beth Stackpole, *Bringing Transparency to the Data Used to Train Artificial Intelligence*, MIT SLOAN (Mar. 3, 2025), <https://mitsloan.mit.edu/ideas-made-to-matter/bringing-transparency-to-data-used-to-train-artificial-intelligence> [<https://perma.cc/8JHU-SKG1>].
- ²⁹ DATA PROVENANCE INITIATIVE, <https://www.dataprovenance.org/> (last visited Aug. 20, 2026).
- ³⁰ About Coalition for Content Provenance and Authenticity (C2PA), C2PA, <https://c2pa.org/about> [<https://perma.cc/5JXZ-X8Z6>] (last visited Aug. 19, 2026).
- ³¹ Stephane Boghossian, *Human-in-the-Loop AI: The Definitive Guide for Lawyers* (2026), HAQQ (May 12, 2026), <https://www.haqq.ai/blog/human-in-the-loop-legal-ai> [<https://perma.cc/EXH4-Z9JS>].
- ³² Ibid. See Nicola Anthony & James Noon.
- ³³ Ibid. See N.Y.C. Bar Ass’n Comm. on Pro. Ethics, Formal Op. 2025-6.
- ³⁴ NATIONAL COURT REPORTERS ASS’N, *NCRA Artificial Intelligence (AI) Position Statement* (Feb. 24, 2026), https://www.ncra.org/docs/default-source/uploadedfiles/operations/ncra-notices/ncra-ai-statement_feb_26_2026.pdf?sfvrsn=4220cbff_5 [<https://perma.cc/CNZ8-DUV2>].
- ³⁵ Heidi Davoren, *Court Transcription Company VIQ Solutions to Be Shut Down, Mass Redundancies Expected*, ABC NEWS (June 5, 2026), <https://www.abc.net.au/news/2026-06-05/viq-solutions-australia-court-transcription-winding-down/106763466> [<https://perma.cc/WCX8-UFDW>].
- ³⁶ EU AI Act: *First Regulation on Artificial Intelligence*, EUR. PARLIAMENT (last updated Feb. 19, 2025), <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> [<https://perma.cc/HZZ7-RNG2>].
- ³⁷ NAT’L INST. OF STANDARDS & TECH., *ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0)* (2023), <https://doi.org/10.6028/NIST.AI.100-1> [<https://perma.cc/AU5Q-KYX4>].
- ³⁸ INT’L ORG. FOR STANDARDIZATION & INT’L ELECTROTECHNICAL COMM’N, *ISO/IEC 42001:2023—INFORMATION TECHNOLOGY—ARTIFICIAL INTELLIGENCE—MANAGEMENT SYSTEM* (2023), <https://www.iso.org/standard/81230.html> [<https://perma.cc/TAR3-KX92>].
- ³⁹ MODEL RULES OF PROFESSIONAL CONDUCT r. 1.1 cmt. 8, rr. 1.4, 1.6, 5.3 (AM. BAR ASS’N).
- ⁴⁰ FED. R. CIV. P. 30(b)(3), 80.
- ⁴¹ *AI & the Courts: Recent Developments*, AM. BAR ASS’N (Apr. 23, 2026), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/april-26-wl/ai-in-the-courts-update-0426wl (PDF on file with author).