

FELICE JOHN VITI, Acting United States Attorney (7007)  
JOEL A. FERRE, Assistant United States Attorney (7517)  
Office of the United States Attorney  
111 Main Street, Suite 1800  
Salt Lake City, Utah 84111  
(801) 325-3317  
joel.ferre@usdoj.gov

---

UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

---

UNITED STATES OF AMERICA,  
*ex rel.*, MICHAEL D. KHOURY,

Plaintiffs,

v.

INTERMOUNTAIN HEALTHCARE, INC.  
d/b/a INTERMOUNTAIN HEALTHCARE,  
*et al.*,

Defendants.

**UNITED STATES' UNOPPOSED  
MOTION TO INTERVENE AND  
DISMISS  
[ECF NO. 307]**

Case No. 2:20-cv-00372-TC-CMR

Judge Tena Campbell  
Magistrate Judge Cecilia M. Romero

---

Pursuant to 31 U.S.C. § 3730(c)(2)(A) of the False Claims Act and Rule 41(a)(2) of the Federal Rules of Civil Procedure, the United States moves to intervene for good cause in this action brought under the *qui tam* provisions of the False Claims Act, 31 U.S.C. §§ 3729-3733, for the purpose of dismissal. The United States believes that continued litigation of this action would not serve the Government's interests and respectfully moves to dismiss this case with prejudice to Relator and without prejudice to the United States. The United States has conferred with Relator and Defendants, and neither opposes the motion.

On June 16, 2020, Relator filed this *qui tam* action against Mountain West Anesthesia ("MWA"), a Salt Lake City-based anesthesiology practice, alleging that MWA anesthesiologists

used personal electronic devices to attend to personal matters while providing general anesthesia services to patients in the operating room and that the anesthesiology services therefore did not meet the accepted standards of medical practice and were not “reasonable and necessary.” *See* 42 U.S.C. § 1395y(a)(1)(A). The United States investigated Relator’s allegations and declined to intervene. Dkt. 19. Relator pursued litigation following the government’s declination. Dkt. 52.

The United States now moves to dismiss this action pursuant to Section 3730(c)(2)(A), which permits the United States to “dismiss the action notwithstanding the objections of the person initiating the action,” if that person “has received notice of the motion and an opportunity for a hearing.” 31 U.S.C. 3730(c)(2)(A); *United States ex rel. Polansky v. Exec. Health Res., Inc.*, 599 U.S. 419, 426 (2023). To dismiss a *qui tam* action in which the United States initially declined to intervene, the United States must first intervene for “good cause” under Section 3730(c)(3). *Id.* 425-426. The Court then evaluates the government’s request for dismissal under Fed. R. Civ. P. 41(a). *Polansky*, 599 U.S. at 436. In practice, “the same grounds that support dismissal also provide good cause to intervene,” *United States ex rel. Carver v. Physicians Pain Specialists of Ala., P.C.*, 2023 WL 4853328, at \*6 (11th Cir. July 31, 2023), so the singular applicable standard here is set out in Federal Rule 41.

Because MWA has filed an answer, Fed. R. Civ. P. 41(a)(2) provides that dismissal may be granted “on terms the court considers proper.” However, in the context of Section 3730(c)(2)(A), application of Rule 41 “will differ in two ways from the norm.” *Polansky*, 599 U.S. at 436-437. First, the court should assess whether the relator has had the “opportunity for a hearing on the motion” required by Section 3730(c)(2)(A). *Id.* Second, the court should consider the relator’s interests in determining whether dismissal is proper, while recognizing that “the Government’s views are entitled to substantial deference.” *Id.* at 437-438.

In this case, the United States has determined that continued litigation of this *qui tam* action is not in the government's interests. The United States has notified Relator of its intent to file this motion and the basis for the motion, and Relator does not object to the motion or the relief sought. Defendants also do not oppose dismissal. Accordingly, good cause exists for the United States to intervene in this *qui tam* action under Section 3730(c)(3) and to dismiss this action under Section 3730(c)(2)(A). The United States requests that the Court enter the attached Proposed Order dismissing this *qui tam* action with prejudice as to Relator and without prejudice as to the United States.

Dated: September 29, 2025

Respectfully submitted,

BRETT SHUMATE  
Assistant Attorney General  
BRENN A JENNY  
Deputy Assistant Attorney General

FELICE JOHN VITI  
Acting United States Attorney

/s/ Joel A. Ferre  
JOEL A. FERRE  
Assistant United States Attorney

JAMIE A. YAVELBERG  
EDWARD C. CROOKE  
SARAH A. HILL  
Attorneys, Civil Division,  
Commercial Litigation Branch  
U.S. Department of Justice  
Post Office Box 261  
Washington, D.C. 20044  
(202) 353-1079

*Counsel for the United States of America*

---

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

---

UNITED STATES OF AMERICA,  
ex rel., MICHAEL D. KHOURY, M.D.,

Plaintiffs,

v.

INTERMOUNTAIN HEALTHCARE, INC.  
d/b/a INTERMOUNTAIN HEALTHCARE,  
et al.,

Defendants.

**ORDER DISMISSING CASE**

Case No. 2:20-cv-00372-TC-CMR

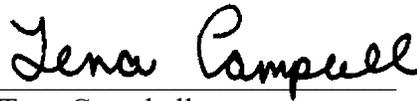
Judge Tena Campbell  
Magistrate Judge Cecilia M. Romero

---

Based on the unopposed Motion to Intervene and Dismiss (ECF No. 306) and for good cause appearing, IT IS ORDERED that the United States' Motion to Intervene and Dismiss is GRANTED. This action is dismissed with prejudice as to Relator and without prejudice as to the United States.

DATED this 30th day of September, 2025.

BY THE COURT:



Tena Campbell  
United States District Judge

# Attys Must Pay \$24K For AI Citations In FIFA Antitrust Case

By **Lauren Berg**

Law360 (September 23, 2025, 10:54 PM EDT) -- Counsel representing the now-shuttered Puerto Rico Soccer League in its antitrust suit against FIFA must pay more than \$24,000 in attorney fees and litigation costs to the soccer federation and other defendants for filing briefs that appeared to contain errors hallucinated by artificial intelligence, a federal judge ruled Tuesday.

U.S. District Judge Raúl M. Arias-Marxuach's **order** partially grants motions brought by FIFA, its local affiliate Federación Puertorriqueña de Fútbol, and Confederation of North, Central America and Caribbean Association Football, which **had asked for** nearly \$88,000 in attorney fees, after the judge in April sanctioned Ibrahim Reyes of Reyes Lawyers PA and his former co-counsel, Jose R. Olmo-Rodriguez of Olmo & Rodriguez Matias Law Office PSC, for using AI to help write briefs.

Noting that the defendants asked for a "significant amount" of fees, the judge cut down the requested amounts to \$12,401 to FIFA, \$6,732 to CONCACAF and \$5,357 to FPF, for a total bill of \$24,492, according to the order.

"The court concludes that some of the hours for which defendants seek fees are too generic or vague for the court to assess if the time billed was appropriate," Judge Arias-Marxuach said. "The does not doubt that these entries accurately represent time spent working on this case but cannot evaluate the reasonableness of the billing due to a lack of detail."

"Most of the problematic entries involved block-billing, where so many tasks were logged for a single block of time such that the court could not determine the reasonableness of time spent expended on these tasks," he added, reducing each block-billed time entry by 30%.

In addition, the judge reduced by 30% the entries he found to be too vague, according to the order.

Judge Arias-Marxuach noted that the plaintiffs' problematic motions included at least 55 erroneous citations, "requiring hours of work on the court's end to check the accuracy of each citation," the order states.

"Plaintiffs' counsel never offered a satisfactory explanation for why their citations in multiple motions were so severely flawed," the judge said. "Plaintiffs denied using generative artificial intelligence. But the sheer number of inaccurate or nonexistent citations suggests otherwise."

"And in any event, the violations of [Federal Rule of Civil Procedure] 11 and applicable ethical rules occurred regardless of whether they were caused by misuse of generative artificial intelligence or other means," he added.

The judge then reduced the initial lodestar amount by 60%, commenting that it wouldn't impose an unreasonable or unnecessary sanction, but he cautioned plaintiffs' counsel and other attorneys in his court "from engaging in similar misbehavior in the future."

Counsel for the parties did not immediately respond to requests for comment Tuesday.

In the underlying case, PRSL alleges that it was the island's top league until it was forced to shut down by allegedly anticompetitive conduct that included FIFA prohibiting the authorization of league tournaments not run by FPF and barring clubs and teams from participating in unauthorized events.

Judge Arias-Marxuach has **preserved the core** antitrust allegations while nixing the suit's fraud claims. PRSL **in June filed** its fourth amended complaint, eliminating previously dismissed claims under the Racketeer Influenced Corrupt Organizations Act, among other claims.

The judge **in April disqualified** plaintiffs' attorney Olmo-Rodríguez from the case, saying he cannot simultaneously be a plaintiff, counsel and factual witness. He said that, while hybrid representation is sometimes allowed, it is not guaranteed and should happen sparingly.

The plaintiffs are represented by Ibrahim Reyes of Reyes Lawyers PA.

FIFA is represented by Roberto A. Cámara-Fuertes and Suleicka Tulier-Vázquez of Ferraiuoli LLC and H. Christopher Boehning and Tiana Voegelin of Paul Weiss Rifkind Wharton & Garrison LLP.

Federación Puertorriqueña de Fútbol is represented by Jose E. Nassar Veglio and Gorman A. Hatcher-Santaella of Pirillo Law LLC.

Confederation of North, Central America and Caribbean Association Football is represented by Anibal A. Román-Medina and Salvador J. Antonetti-Stutts of O'Neill & Borges LLC and Amanda M. Blau, John J. Kuster and Jon Muenz of Sidley Austin LLP.

The case is Puerto Rico Soccer League NFP Corp. et al. v. Federación Puertorriqueña de Fútbol Inc. et al., case number 3:23-cv-01203, in the U.S. District Court for the District of Puerto Rico.

--Additional reporting by Madison Arnold, Bryan Koenig and Elaine Briseño. Editing by Jay Jackson Jr.

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ALABAMA  
SOUTHERN DIVISION**

<b>FRANKIE JOHNSON,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	<b>Case No.: 2:21-cv-1701-AMM</b>
	)	
<b>JEFFERSON S. DUNN, et al.,</b>	)	
	)	
<b>Defendants.</b>	)	
	)	

**SANCTIONS ORDER**

This case is before the court because incarcerated Plaintiff Frankie Johnson accused Defendant Jefferson Dunn, the former Commissioner of the Alabama Department of Corrections, of fabricating citations to legal authorities in two motions. Docs. 187, 193. Three attorneys for Defendant Dunn (Matthew B. Reeves, William J. Cranford, and William R. Lunsford) confirmed in writing and at a hearing that the citations were hallucinations of a popular generative artificial intelligence (“AI”) application, ChatGPT. *See* Docs. 194, 200. In simpler terms, the citations were completely made up.

The court must determine an appropriate sanction. Fabricating legal authority is serious misconduct that demands a serious sanction. In the court’s view, it demands substantially greater accountability than the reprimands and modest fines that have become common as courts confront this form of AI misuse. As a practical

matter, time is telling us – quickly and loudly – that those sanctions are insufficient deterrents. In principle, they do not account for the danger that fake citations pose for the fair administration of justice and the integrity of the judicial system. And in any event, they have little effect when the lawyer’s client (here, an Alabama government agency) learns of the attorney’s misconduct and continues to retain him.

An appropriate and reasonable sanction must (1) have sufficient deterrent force to make this misuse of AI unprofitable for lawyers and litigants, (2) correspond to the extreme dereliction of professional responsibility that sham citations reflect (whether generated by artificial or human intelligence), and (3) effectively communicate that made-up authorities have no place in a court of law.

For the reasons explained below, the court **PUBLICLY REPRIMANDS** Mr. Reeves, Mr. Cranford, and Mr. Lunsford for making false statements to the court; **ORDERS** publication of this order to effectuate that reprimand; **DISQUALIFIES** them from further participation in this case; and **REFERS** this matter to the Alabama State Bar and other applicable licensing authorities.

In the light of the results of the independent investigation commissioned by the attorneys’ law firm, the court exercises its discretion not to suspend them from practice in the Northern District of Alabama. The court **RELEASES WITHOUT SANCTION** attorneys Daniel J. Chism and Lynette E. Potter, and the law firm Butler Snow LLP (“Butler Snow”) from disciplinary proceedings.

## I. BACKGROUND

### A. Procedural Background

On May 7, 2025, Defendant Dunn filed a motion for leave to take the deposition of an incarcerated person under Federal Rule of Civil Procedure 30(a)(2)(B), which is required to depose any incarcerated person. Doc. 174. The signature block of that motion contained the names of four attorneys from the Butler Snow law firm: William J. Cranford, William R. Lunsford, Matthew B. Reeves, and Daniel J. Chism. *Id.* at 4. Mr. Cranford electronically filed the motion with his filing credentials. Plaintiff Johnson, the incarcerated person at issue, objected to being deposed prior to receipt of certain documents from the Alabama Department of Corrections that were the subject of a motion to compel by him. Doc. 186 at 2; *see also* Doc. 169. All parties agreed that Plaintiff Johnson was due to be deposed; the dispute was simply about when (Defendant Dunn wanted to conduct the deposition the week of June 3rd and Plaintiff Johnson wanted sometime later, after receipt of the documents at issue in his motion to compel).

On May 8, 2025, Defendant Dunn sought leave of court to file a motion to compel interrogatory answers and document production from Plaintiff Johnson. Doc. 178. The next day, the court granted that leave. Doc. 179. At 11:21 a.m.<sup>1</sup> on May 12, 2025, Defendant Dunn filed an unopposed motion for excess pages as to

---

<sup>1</sup> All times noted in this order are in Central Daylight Time.

the forthcoming motion to compel. Doc. 180. The court granted the motion for excess pages at 12:39 p.m. Doc. 181. Then, at 4:21 p.m. on May 12, 2025, Defendant Dunn filed his motion to compel. Doc. 182. Four Butler Snow attorneys appeared on the signature block of that motion: Mr. Cranford, Mr. Lunsford, Mr. Reeves, and Ms. Potter. *Id.* at 20. Ms. Potter has not entered a notice of appearance in this case.

Plaintiff Johnson's motion to compel became fully briefed on May 12, 2025. *See* Doc. 183. On May 14, 2025, the court granted in part and denied in part Plaintiff Johnson's motion to compel. Doc. 184.

The next day, Plaintiff Johnson filed a response to the motion for leave to depose him. Doc. 186. Plaintiff Johnson objected to a deposition the week of June 3rd on several grounds, including that counsel for Defendant Dunn appeared to have fabricated citations to legal authority in his motion for leave and motion to compel, "possibly through the use of generative artificial intelligence." *Id.* at 1.

In total, there were five problematic citations across two motions:

- Defendant Dunn cited "United States v. Baker, 539 F. App'x 937, 943 (11th Cir 2013)" as "confirming broad discovery rights under Rules 26 and 30." Doc. 174 at 2. As Plaintiff Johnson pointed out, "[w]hile *United States v. Baker*, 529 Fed. Appx. 987 (11th Cir. 2013) is an actual case, it is an appeal challenging a criminal's sentencing enhancement." Doc. 186 at 2. And the case found in the Federal Appendix numbers cited by Defendant Dunn does not discuss discovery. *See Williams v. Morahan*, 539 F. App'x 937 (11th Cir. 2013).
- Defendant Dunn cited "Kelley v. City of Birmingham, 2021 WL 1118031, at \*2 (N.D. Ala. Mar. 24, 2021)" for the proposition that the district court "refus[ed] to delay deposition based on unrelated discovery issues."

Doc. 174 at 2. The only case with that style which Plaintiff Johnson (and the court) could find was an Alabama Court of Appeals case from 1939 that dealt with a traffic offense. Doc. 186 at 3; *see Kelley v. City of Birmingham*, 28 Ala. App. 644, 189 So. 921 (Ala. Ct. App. 1939).

- Defendant Dunn cited “Greer v. Warden, FCC Coleman I, 2020 WL 3060362, at \*2 (M.D. Fla. June 9, 2020)” as “rejecting inmate’s request to delay deposition until additional discovery was completed.” Doc. 174 at 2. This case does not exist, nor does a case exist with a similar citation for that proposition of law. *See* Doc. 186 at 3.

- Defendant Dunn cited “Wilson v. Jackson, 2006 WL 8438651, at \*2 (N.D. Ala. Feb. 27, 2006)” with the parenthetical that it was an opinion “granting [a] Rule 30(a)(2)(B) motion and finding no good cause to delay deposition of incarcerated plaintiff.” Doc. 174 at 2. There is no such case, and that Westlaw number directs to a maritime personal injury case that does not discuss discovery. *See Douglas v. Ingram Barge Co.*, No. CV 3:04-0383, 2006 WL 8438651 (S.D.W. Va. Sept. 15, 2006); *see also* Doc. 186 at 4.

- Defendant Dunn cited “Williams v. Asplundh Tree Expert Co., No. 3:05-cv-479, 2006 WL 3343787, at \*4 (M.D. Fla. Nov. 17, 2006)” to support the statement that, “General objections are not useful and will not be considered by the Court. Objections should be specific and supported by a detailed explanation.” Doc. 182 at 13. Though a case with that style exists, no case with that combination of style and proposition exists. *See Williams v. Asplundh Tree Expert Co.*, No. 3:05-cv-00479-VMC-MCR (M.D. Fla. July 23, 2013); *see also* Doc. 186 at 4.

At 12:14 p.m. on Friday, May 16, 2025, the court issued a show cause order noting that “[i]n the light of the seriousness of the accusation, the court ha[d] conducted independent searches for each allegedly fabricated citation, to no avail,” and ordering the signatories of Defendant Dunn’s motion for leave, and the Butler Snow law firm, “to show good cause, if there be any, why they should not be sanctioned under Federal Rule of Civil Procedure 11, the court’s inherent authority,

Local Rule 83.1(f), and/or Alabama Rule of Professional Conduct 3.3 for making false statements of fact or law to the court, not later than 3:00 PM Central Daylight Time on Monday, May 19, 2025.” Doc. 187 at 1–2 (emphasis omitted). The court also set a show cause hearing for 9:00 a.m. Central Daylight Time on Wednesday, May 21, 2025 at the Hugo Black United States Courthouse. *Id.* at 2.

Three hours after the order to show cause issued, Mr. Lunsford and Mr. Chism filed a motion to be excused from the show cause hearing. Doc. 188. Mr. Chism and Mr. Lunsford represented that “[n]either [of them] participated in any way in the drafting or filing of the Motion for Leave to Depose Incarcerated Persons,” and that Mr. Lunsford “must be in Macon, Georgia to [] prepare for and attend a previously set evidentiary hearing before the U.S. District Judge Marc Treadwell in the United States District Court for the Middle District of Georgia.” *Id.* at 2.

The court denied their requested excuse at 6:39 p.m. that same day:

The hearing before Judge Treadwell is set for Thursday, May 22, 2025, at 9:00 AM Eastern Standard Time—twenty-three hours after the show cause hearing in this case. *See Ricardo Daughtry, et al. v. Shawn Emmons, et al.*, No. 5:15-cv-00041-MTT (M.D. Ga. filed Feb. 12, 2015). The May 21, 2025 show cause hearing will last no longer than an hour. Accordingly, Mr. Lunsford will have ample time to travel to Georgia in advance of his hearing the next day, and the motion to excuse as to Mr. Lunsford and Mr. Chism is **DENIED**.

Doc. 190 at 2. Several attorneys representing other parties sought and received excuses from the show cause hearing. Docs. 189–92, 196–97.

On Monday, May 19, 2025, the court issued a supplemental show cause order:

Out of an abundance of caution, the court **CLAIRIFIES** its show cause order to the extent that (1) Defendant Dunn’s motion to compel is also the subject of that show cause order and will be discussed at the hearing set for Wednesday, May 21, 2025 at 9:30 AM Central Daylight Time, and (2) in addition to the four attorneys on the motion for leave, Ms. Lynette E. Potter is **ORDERED** to show good cause, if there be any, why she should not be sanctioned under Federal Rule of Civil Procedure 11, the court’s inherent authority, Local Rule 83.1(f), and/or Alabama Rule of Professional Conduct 3.3 for making false statements of fact or law to the court.

Doc. 193 at 2–3.

Later that day, Mr. Lunsford, Mr. Reeves, Mr. Cranford, and Mr. Chism filed their response to the show cause orders, admitting that the citations were hallucinated by ChatGPT: “In short, attorney Matt Reeves used ChatGPT to obtain case citations in support of two arguments made in the motions at issue without verifying their accuracy, and those citations proved to be false.” Doc. 194 at 1. The response included declarations from each attorney. *See* Docs. 194-1–4.

Butler Snow then filed its response, called the events “unacceptable,” and requested that “that any sanctions be proportionate to the wrong and commensurate with each attorney’s role in these events,” “that its client not be sanctioned, and for counsel to have the opportunity to file an amended motion with correct citations.” Doc. 195 at 1–2. Ms. Potter later filed her response, Doc. 198, and a declaration, Doc. 198-1.

The court held the show cause hearing on May 21, 2025. Doc. 200. Counsel of record who were not previously excused, representatives from Butler Snow, and

a representative from the Alabama Attorney General’s Office appeared.

Following the show cause hearing, the court allowed “supplemental responses to the order to show cause and briefs from anyone else who wishe[d] to file [one].” Doc. 199. Additionally, the court granted leave for Defendant Dunn to file corrected versions of the motions at issue, which he later filed. *See* Docs. 201–02. Butler Snow filed a supplemental response to the show cause orders on June 2, 2025. Doc. 203.

## **B. The Attorneys**

Mr. Lunsford, Mr. Reeves, Mr. Cranford, Mr. Chism, and Ms. Potter spoke at the show cause hearing and filed supplemental declarations. Docs. 200, 203-3–7.

### **1. William J. Cranford**

Mr. Cranford is of counsel at Butler Snow. Doc. 194-3 ¶ 2. As to the motion for leave to depose, Mr. Cranford stated in his initial declaration that: (1) he “drafted the initial version of Dunn’s Motion for Leave to Depose Incarcerated Persons”; (2) he “submitted the draft Motion for Leave for review to [his] direct supervisors, Matt Reeves, and Bill Lunsford” while copying Mr. Chism; (3) “[o]n May 7, 2025, Matt Reeves returned revisions to the draft Motion for Leave to [him]” and that “[t]he revisions included the string citation at issue . . . in paragraph two of the Motion for Leave”; (4) although he “reviewed [the edits] for grammatical and typographical issues, [he] did not conduct an independent review of the legal authorities added” and “incorporated the . . . revisions into a final draft of the Motion for Leave for

filing with the Court”; (5) “[u]pon approval from Matt Reeves, [he] electronically signed and filed the Motion for Leave on May 7, 2025”; and (6) he “possessed no knowledge that Matt Reeves utilized generative artificial intelligence to generate these citations when [he] filed the Motion.” *Id.* ¶¶ 4–9.

As to the motion to compel, Mr. Cranford stated in his initial declaration that: (1) he “drafted the initial version of the Motion to Compel”; (2) “[o]n May 10, 2025, [he] submitted the draft Motion to Compel for review to [his] direct supervisors, Matt Reeves, and Bill Lunsford, and copied Daniel Chism”; (3) “[o]n May 11, 2025, Matt Reeves returned revisions to the draft Motion to Compel to [him]” and “included the block citations located on page thirteen of the Motion to Compel”; (4) that same day, “after receiving the revisions, [he] reviewed them for grammatical and typographical issues,” but “did not conduct an independent review of the legal authorities added” and “incorporated the . . . revisions into a final draft of the Motion to Compel”; (5) he “submitted the revised Motion to Compel to Matt Reeves and Bill Lunsford for final approval on May 11, 2025, and received no further revisions”; (6) he “electronically signed and filed the Motion to Compel on May 12, 2025”; (7) “at the time of filing, [he] lacked any knowledge that Matt Reeves utilized generative artificial intelligence to generate the[ problematic] citations”; and (8) he “erroneously included Lynette Potter in the signature block of the Motion to Compel for the Butler Snow attorneys of record in the case.” *Id.* ¶¶ 12–14, 17–21.

At the show cause hearing, Mr. Cranford apologized and “accept[ted] full responsibility.” Doc. 200 at 18. He described his understanding of that responsibility: “I signed these motions. I understand that by signing these motions, I was verifying and accepting responsibility for the contents of those motions. And I take full responsibility for that. There’s no excuse for not verifying these citations . . .” *Id.* at 18–19. He also described his practice for edits from supervisors:

[I]n my normal practice, when I submit a draft to Mr. Reeves or Mr. Lunsford, if I receive revisions back, my typical practice is to incorporate those revisions, make sure they are factually accurate for the case since I usually have a more detailed understanding of the facts and the history, background of the case, and check for typographical or grammatical errors. In my normal practice, I do not typically check citations that are added from Mr. Lunsford or Mr. Reeves.

*Id.* at 19. Mr. Cranford represented that when he received the edits from Mr. Reeves, the edits in the motion for leave to depose were in redline and the edits in the motion to compel were in plain text. *Id.* at 19–20. He further represented that he was “unaware of any other instances of lawyers with [his] group using ChatGPT or an outside AI source for legal research or drafting of a legal document” besides Westlaw’s CoCounsel product. *Id.* at 20.

In a supplemental declaration, Mr. Cranford stated that he has “never used any publicly accessible, generative artificial intelligence chatbot, such as OpenAI’s ChatGPT, to generate legal or other authority citations for submission to any court.” Doc. 203-5 ¶ 2.

Mr. Cranford did not have a “specific position” on an appropriate sanction other than to say that it is “within [the court’s] discretion” and that he “accept[s] whatever the Court deems to be appropriate in this instance.” Doc. 200 at 20–21.

## 2. Matthew B. Reeves

Mr. Reeves is a partner and assistant practice group leader in Butler Snow’s constitutional and civil rights litigation group. Doc. 195 at 2. He stated in his declaration that: (1) he was “responsible for revising Paragraph 2 of the Motion for Leave and Page 13 of the Motion to Compel, including the legal authorities cited therein”; (2) he “performed a search [on ChatGPT] to identify supporting case law for the proposition that discovery may proceed even during the pendency of other discovery issues, as to the Motion for Leave, and that general or boilerplate objections are not effective, as to the Motion to Compel”; (3) he “failed to verify the case citations returned by ChatGPT through independent review in Westlaw or PACER before including them in the Motion for Leave and Motion to Compel”; and (4) that the citations at issue are inaccurate or do not exist. Doc. 194-2 ¶¶ 3–5. Mr. Reeves further stated that this “was a serious error in judgment, and contrary to the requirements of Butler Snow LLP and [his] obligations to this Court.” *Id.* ¶ 6.

At the show cause hearing, Mr. Reeves stated that he has “had limited use” “with various AI products” “since approximately March of 2024.” Doc. 200 at 21. Besides Westlaw’s CoCounsel product, Mr. Reeves stated that he used ChatGPT. *Id.* at 21–

22. He “initially used [ChatGPT] for personal reasons, to look up things related to dietary-related matters,” “to look up things when [his family went] on trips,” “and when [his] youngest son started looking at colleges, doing some research on that for colleges and universities.” *Id.* Then, he began using ChatGPT professionally. *Id.* at 22. Mr. Reeves gave examples of “basic” tasks such as “a general search of any sort of background, history kind of stuff” for “a witness that was going to be deposed” or “to go get a survey of what was out there publicly available . . . to get an idea of what the body of policies in the corrections world looked like.” *Id.* He also stated that he “was aware of the limitation on use [of artificial intelligence products at Butler Snow]; and in this instance . . . [he] did not comply with the [firm’s] policy,” and that these are “the two instances” in which he used artificial intelligence and “did not verify the citations.” *Id.* at 23.

In a supplemental declaration, Mr. Reeves stated that “[e]xcept in the motions already subject to the Court’s Order to Show Cause,” he has “never used any publicly accessible, generative artificial intelligence chatbot, such as OpenAI’s ChatGPT, to generate legal or other authority citations for submission to any court.” Doc. 203-4 ¶ 2. In addition, Mr. Reeves stated that he is working with Anil Mujumdar, counsel for Plaintiff Johnson and a professor at the University of Alabama School of Law, to develop “an informative program to educate law students regarding the risks of AI.” *Id.* ¶¶ 3–4. Mr. Reeves “intend[s] to pursue this program and a similar program

at Samford University’s Cumberland School of Law and Faulkner University’s Thomas Goode Jones School of Law regardless of whether the Court orders it as relief in this case.” *Id.* ¶ 5.

Mr. Reeves’s position on sanctions “is that [he] understand[s] it is well within [the court’s] discretion to provide whatever sanction [the court] deem[s] appropriate,” and because he is “the one responsible for the error,” he hopes that the court “would not punish [his] colleagues for that.” Doc. 200 at 24.

### **3. William R. Lunsford**

Mr. Lunsford is a partner and practice group leader of the constitutional and civil rights litigation group at Butler Snow. Doc. 194-1 ¶ 3. Mr. Lunsford began his initial declaration by “apologiz[ing] to the Court, to all parties, to opposing counsel and to the State of Alabama for the terrible decisions that led to an erroneous filing.” *Id.* ¶ 2. He also stated that “[u]pon receipt of the Court’s [show cause] Order (Doc. No. 187), [he] promptly contacted the Commissioner of the Alabama Department of Corrections, the General Counsel for the Department of Corrections and the Chief Counsel for the Attorney General to inform them of the Court’s Order.” *Id.* ¶ 5.

At the show cause hearing, the court asked about Mr. Lunsford’s motion to be excused:

THE COURT: . . . When you filed your motion to be excused, I think a few hours had elapsed since I had issued the show cause order.

Had you at the time you filed the motion to be excused performed any

work to understand the extent or nature of the hallucinated citations or whether there might be any other such citations in this case or in others?

MR. LUNSFORD: The short answer is no, Your Honor. It was filed quickly in haste on a Friday afternoon when I did not appreciate the full context of the Court's order.

Doc. 200 at 25.

In his declaration, Mr. Lunsford also described his role in representing the Alabama Department of Corrections and the State of Alabama:

I have had the honor of representing the Alabama Department of Corrections and its officials in various capacities (i.e. as directly retained counsel or counsel retained by third party contractors under indemnity obligations) over more than twenty (20) years. My name and signature appear on all of the current public contracts for professional services provided by outside legal counsel to the State of Alabama (the "State") on a limited number of matters for which the State elects to hire outside counsel. As such, I am the principal responsible attorney for all matters currently assigned to the firm regarding the Alabama Department of Corrections ("ADOC"). As a general matter, we have been retained to represent the State in systemic reform litigation brought against ADOC as well as a small number of individual plaintiff cases with a factual nexus to our pending systemic reform matters. I, along with my partner Matt Reeves, routinely monitor the assignment of attorneys within our firm to our matters for the State and its Department of Corrections in effort to effectively manage the representation of the State in each assigned matter.

For purposes of representing current and former ADOC officials in the individual plaintiff classes, such as the Johnson matter, we routinely assign one or two younger attorneys to the matter with Matt Reeves and I providing supervisory coverage. Due to the nature of our cases and work, Matt Reeves provides more of the day-to-day oversight, supervision and direction on the individual plaintiff's cases filed against current and/or former ADOC officials; however, I also provide supervision – particularly in times when the demands of our other cases or clients or personal events render Matt unavailable. Dan Chism and

Will Cranford have been primarily assigned to represent ADOC and its current and former officials in the individual plaintiff cases since they began working with us more than two (2) years ago.

Doc. 194-1 ¶¶ 7–8; *see also* Doc. 200 at 25–26 (show cause hearing transcript).

As to the motion for leave to depose, Mr. Lunsford stated that he did not review the draft due to other work obligations. Doc. 194-1 ¶ 9. Mr. Lunsford stated that he did review the motion to compel:

As with the Motion for Leave, Will Cranford drafted the initial Motion to Compel and he transmitted the draft to Matt Reeves for review at 11:43 a.m. on Saturday, May 10, 2025. Matt responded with revisions to the original draft at approximately 2:45 a.m. on Sunday, May 11, 2025. Will recirculated another draft of the Motion to Compel incorporating the revisions of Matt Reeves at 7:29 p.m. on Sunday, May 18, 2025. I briefly scanned the document on Sunday night and responded to Will via email within approximately fifteen minutes, indicating that I did not have any changes. My brief review focused more on the facts outlined as the basis for the motion to compel and the bolded headings of the legal arguments. I did not conduct any detailed or substantive review of the legal authorities. Given that the document had already undergone a review by Matt Reeves, I did not conduct any level of detailed review. I certainly did not conduct the level of detailed review that I would otherwise conduct if I was the sole reviewing attorney. Moreover, from my personal experiences with Will Cranford over the last two years, he has consistently demonstrated proficiency in promptly incorporating written feedback from his supervising attorneys and, as such, I did not have significant concerns about Will’s incorporation of the changes provided by Matt Reeves.

*Id.* ¶ 10.

Mr. Lunsford described Mr. Reeves adding legal citations as a supervisory attorney to be “atypical” and “rare” in their group practice. *Id.* ¶ 11. He further stated:

[O]ur historical process creates an expectation and mutual

understanding that the attorney crafting and adding legal authorities ensures their accuracy and, as such, I would not have expected Will Cranford to conduct such a review of a senior, supervisory attorney's additional legal arguments or authorities. Finally, this is the only instance in over a decade of working with Matt Reeves when I have ever encountered an instance when he added a citation that he failed to validate.

*Id.*

At the show cause hearing, when the court asked Mr. Lunsford to provide the “basis for [his] expectation that Mr. Cranford would have affixed his signature to the motions without reviewing the additional citations,” Mr. Lunsford stated that “much of the law” and “much of the precedent” between the cases he oversees are “the same” “so there are a lot of occasions when Matt [Reeves] or [he] will see authority and/or see a place where authority might be missing and go pull from [their] other available resources and plug that into the document.” Doc. 200 at 27. “And so the practice, the cadence that’s developed over [almost fifteen years] is most of everything [Mr. Reeves or Mr. Lunsford] pull is from another brief or another previous writing where [they] know other authority exists.” *Id.*

In his declaration, Mr. Lunsford described Butler Snow’s “proactive” approach to artificial intelligence:

[Butler Snow] has been proactive in investigating, warning against and attempting to establish firm guidance on the use of the ever-evolving availability of products generated utilizing artificial intelligence. Under firm policy, the use of ChatGPT for legal research requires written approval from a practice group leader. I have yet to receive or approve any such request. I can state with certainty that our Firm has made the

limitations upon the use of artificial intelligence abundantly clear to all of our attorneys. The conduct reported in this instance flies in the face of known Firm policy, which the Firm will handle internally. Moreover, I was not aware of any of our attorneys relying upon artificial intelligence of any kind to prepare any of our legal filings and I can assure this Court that I along with the leadership of the Firm are revisiting this issue to evaluate ways that we can ensure that these instances do not occur again.

Doc. 194-1 ¶ 12. In addition, at the show cause hearing, Mr. Lunsford stated that his team had discussions about Westlaw’s artificial intelligence program, CoCounsel, and “a discussion when [their] vendor for court reporting transcripts began providing [them], free of charge for a period of time, AI summaries of a deposition.” Doc. 200 at 28–29. Mr. Lunsford recalled that “there was equal parts amazement and concern,” with “an immediate clear recognition that those [deposition] summaries could never be relied upon in drafting any documents.” *Id.* at 29.

Mr. Lunsford represented at the show cause hearing that he “spent probably a collective four hours going through emails and reviewing redlines of drafts that Mr. Reeves had circulated,” and did not find any additional problems like the ones at issue here. *Id.* at 30–31. That review included “three mediation statements,” “a response to a court-monitoring report,” “some smaller motions for leave,” and “some summary judgment motions,” but he also represented that “the firm’s response to this is not complete yet.” *Id.* at 30–33.

In a supplemental declaration, Mr. Lunsford stated that he has “never used any publicly accessible, generative artificial intelligence chatbot, such as OpenAI’s

ChatGPT, to generate legal or other authority citations for submission to any court.”

Doc. 203-3 ¶ 2.

Mr. Lunsford did not have a position on appropriate sanctions that differed from that of Butler Snow. Doc. 200 at 33.

#### **4. Daniel J. Chism**

Mr. Chism is an associate at Butler Snow. Doc. 194-4 ¶ 2. In his declaration, he stated that although he “was copied on emails circulating drafts,” he “did not draft, revise, or review the Motions [at issue].” *Id.* ¶ 4. Mr. Chism reaffirmed that statement at the show cause hearing. Doc. 200 at 17–18. In a supplemental declaration, he stated that he has “never used any publicly accessible, generative artificial intelligence chatbot, such as OpenAI’s ChatGPT, to generate legal or other authority citations for submission to any court.” Doc. 203-6 ¶ 2.

#### **5. Lynette E. Potter**

Ms. Potter is an attorney at Butler Snow. Doc. 198-1 ¶ 2. In her declaration, she stated that she “did not draft, edit, review, supervise, or approve the Motions or any drafts of the Motions,” and “possessed no knowledge related to the preparation or filing of the Motions or any of their contents until May 16, 2025, when the Court entered its Show Cause Order.” *Id.* ¶ 5. Ms. Potter reaffirmed those statements at the show cause hearing. Doc. 200 at 17–18. In a supplemental declaration, she stated that she has “never used any publicly accessible, generative artificial intelligence

chatbot, such as OpenAI’s ChatGPT, to generate legal or other authority citations for submission to any court.” Doc. 203-7 ¶ 2.

### **C. Butler Snow**

Butler Snow filed an initial response, a supplemental response, and had representatives at the show cause hearing. *See* Docs. 195, 200, 203. Benjamin Watson, Butler Snow’s general counsel, represented at the show cause hearing that Butler Snow believes that Mr. Lunsford and Mr. Chism’s motion to be excused from the show cause hearing “should not have been filed” and that the firm was unaware of the motion before it was filed. Doc. 200 at 12–13.

Mr. Watson further represented at the show cause hearing that Butler Snow did not find similar issues in other filings in this case and within “nine filings from . . . three different cases.” *Id.* at 13–14.

Butler Snow expanded this review after the show cause hearing and detailed those efforts in its supplemental response. That “extensive review” included examining “all filings in all Alabama federal courts and the Eleventh Circuit Court of Appeals on or after April 1, 2023, where counsel of record from this case, and also Lynette Potter, appeared on any filing.” Doc. 203 at 1 (footnote omitted). “In total, the Butler Snow team reviewed 52 Alabama federal court dockets; of those, 40 dockets contained substantive citations for review. Butler Snow attorneys examined every citation in those 40 dockets and did not find any additional apparent AI-

generated ‘hallucinations.’” *Id.* at 2 (citations omitted).

Separately, Butler Snow “at its own cost and expense” engaged Morgan, Lewis & Bockius LLP (“Morgan Lewis”) to conduct an independent review. *Id.* at 2 & n.2. A team of twenty-eight attorneys at Morgan Lewis “verif[ied] all citations in those same 40 dockets in Alabama federal courts and the Eleventh Circuit Court of Appeals.” *Id.* at 2. “In all, Morgan Lewis reviewed more than 2,400 separate legal citations across 330 filings.” *Id.*

Scott Milner, a partner at Morgan Lewis, stated in a declaration that the review revealed no additional “legal citations that were fabricated,” nor a legal citation that “was to a legitimate source but did not bear on the proposition for which it was cited.” Doc. 203-2 ¶ 36. Mr. Milner is the practice group leader of the eData Practice Group at Morgan Lewis and has extended his practice “[o]ver the last several years” to artificial intelligence issues. *Id.* ¶¶ 1, 6.

Butler Snow also described its artificial intelligence policies both prior to and in response to this episode. To that end, Mr. Watson filed a declaration. Doc. 195-1. Mr. Watson stated that in June 2023, all Butler Snow attorneys received an email “stating that ‘there are significant risks that LLM [Large Language Model] output can appear perfectly researched and logical while in fact it is wholly inaccurate.’” *Id.* at 2–3, 6. That same email implemented a policy which requires “written permission from the appropriate Practice Group Leader to use this new technology as a

secondary research tool, with full checks of the accuracy of any results through traditional legal research methods.” *Id.* Similarly, when Butler Snow provided its attorneys access to Westlaw’s CoCounsel platform in January 2025, it “adopted and distributed a policy” that “[a]ll outputs must be reviewed and verified by the responsible attorney before being presented to clients, filed with courts, or otherwise relied upon.” *Id.* at 3, 9.

At the show cause hearing, counsel for Butler Snow confirmed that attorneys from the firm had written articles detailing the dangers associated with artificial intelligence in legal work and that, according to Butler Snow’s then-existing policy, practice group leaders did not have to seek permission to utilize artificial intelligence. Doc. 200 at 10–12.

Mr. Watson stated in his initial declaration that Butler Snow has an artificial intelligence committee that is drafting “a comprehensive artificial intelligence policy.” Doc. 195-1 at 3, 11–16. And after this incident, that he “sent a reminder to all Butler Snow attorneys of their ethical and professional duties to verify the accuracy of all citations or other authority presented to any court.” *Id.* at 4, 17.

On a prospective basis, Mr. Watson stated that “Butler Snow will conduct additional and extensive firm-wide training on the appropriate use of artificial intelligence, including training to ensure that any citation to authority, no matter its source, is accurate, truthful, and unquestionably stands for the proposition for which

it is being offered.” *Id.* at 4. In addition, “Butler Snow will be adopting a prefiling protocol requiring (a) review of all legal authority in any document to be filed with a court of law and (b) confirming the existence, accuracy, and relevance of each citation.” *Id.* at 4–5.

Mr. Watson addressed other firm policy issues at the show cause hearing. He told the court that Butler Snow has “no specific policy” as to “who is on the signature block [of a filing] and who should appear and should not appear.” Doc. 200 at 15. Instead, “it is left to the individual lawyer’s discretion in terms of who should be on the signature block.” *Id.* Mr. Watson represented that Butler Snow “need[s] to make clear” that junior attorneys who affix their signatures to a filing “must verify that” filing, even if a senior attorney sends it to them. *Id.* at 15–16.

Mr. Watson stated in his initial declaration that “Butler Snow is ultimately responsible for the acts of its attorneys and is prepared to accept any sanction that the Court deems appropriate, particularly in light of the seriousness of the conduct in this matter.” Doc. 195-1 at 5. Mr. Watson echoed this at the show cause hearing: “So we stand ready to adhere to any sanction that you may deem appropriate.” Doc. 200 at 16. In its supplemental response, Butler Snow made a specific request:

Given the magnitude of the harm, the isolated nature of the harm, the significant publicity given to these events, and the remediation efforts undertaken by Butler Snow and attorney Reeves, Butler Snow respectfully requests that the Court limit any sanctions it may impose to a modest sanction upon it and to the exclusion of the affected clients in this litigation.

Doc. 203 at 5 (footnotes omitted).

Finally, Butler Snow represented that “[t]he State of Alabama will incur no expense or charge of any kind generated or incurred by the firm in connection with the erroneous filings, the proceedings related to those filings, or the remedial actions taken by the firm to respond to this matter, including the fees paid to Morgan Lewis.”

Doc. 203 at 2 n.2.

#### **D. Office of the Alabama Attorney General**

Attorney Brad Chynoweth attended the show cause hearing on behalf of the Alabama Attorney General. Doc. 200 at 7. He expressed that his office is “very concerned,” “want[s] to ensure that there are no other instances of this in any other filings in corrections cases,” and “Mr. Lunsford remains the [A]ttorney [G]eneral’s counsel of choice.” *Id.* at 38–40. Mr. Chynoweth stated that the Attorney General appointed Mr. Lunsford as a deputy attorney general to litigate on behalf of the State and that the “appointment process makes clear that the deputy attorney general can use the services of other attorneys in his firm.” *Id.* at 39.

Mr. Chynoweth also noted that “there is no generative AI platform that is authorized for use” by the Attorney General’s office. *Id.* at 40.

## **II. FINDINGS OF FACT & CONCLUSIONS OF LAW**

Every lawyer knows that citing fake cases in a court filing is a terrible decision. No one here is attempting to defend it. In the few years that generative AI

has affected court filings, it has become well established that “[m]any harms flow from the submission of fake opinions.” *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443, 448 (S.D.N.Y. 2023); *see, e.g., Dehghani v. Castro*, No. 2:25-cv-00052-MIS-DLM, 2025 WL 1361765 (D.N.M. May 9, 2025); *Bevins v. Colgate-Palmolive Co.*, No. 25-576, 2025 WL 1085695 (E.D. Pa. Apr. 10, 2025); *Ferris v. Amazon.com Servs., LLC*, No. 3:24-cv-304-MPM-JMV, 2025 WL 1122235 (N.D. Miss. Apr. 16, 2025); *United States v. Hayes*, 763 F. Supp. 3d 1054 (E.D. Cal. 2025), *reconsideration denied*, No. 2:24-cr-0280-DJC, 2025 WL 1067323 (E.D. Cal. Apr. 9, 2025); *Sanders v. United States*, 176 Fed. Cl. 163 (Fed. Cl. 2025); *Wadsworth v. Walmart Inc.*, 348 F.R.D. 489 (D. Wyo. 2025); *Gauthier v. Goodyear Tire & Rubber Co.*, No. 1:23-cv-281, 2024 WL 4882651 (E.D. Tex. Nov. 25, 2024); *Park v. Kim*, 91 F.4th 610 (2d Cir. 2024).

Some such harms affect the case at hand: “The opposing party wastes time and money in exposing the deception,” and “[t]he client may be deprived of arguments based on authentic judicial precedents.” *Mata*, 678 F. Supp. 3d at 448. While the court takes time to investigate, other cases may be disrupted or deprived of judicial attention. Other harms affect the judicial system:

There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity.

*Id.* at 448–49. And the public (whose taxpayer dollars pay the lawyers at issue here) is justifiably horrified and outraged when filings in a court of law substitute lazy, convenient fictions for the truth.

Even in cases like this one, where lawyers who cite AI hallucinations accept responsibility and apologize profusely, much damage is done. The opposing party expends resources identifying and exposing the fabrication; the court spends time reviewing materials, holding hearings, deliberating about sanctions, and explaining its ruling; the substance of the case is delayed; and public confidence about the trustworthiness of legal proceedings may be diminished.

Accordingly, the court makes the following findings of fact and conclusions of law.

**A. False Statements of Law**

The court finds, based upon its own careful review and as no one contests, that the hallucinated citations in the two motions at issue were false statements of law. *See* Docs. 194, 200.

**B. Sanctions Authorities**

Rule 11(b) provides that “[b]y presenting to the court a pleading, written motion, or other paper[,] . . . an attorney . . . certifies that . . . after an inquiry reasonable under the circumstances . . . the claims, defenses, and other legal contentions are warranted by existing law.” Fed. R. Civ. P. 11(b)(2).

“If, after notice and a reasonable opportunity to respond, the court determines that Rule 11(b) has been violated, the court may impose an appropriate sanction on any attorney, law firm, or party that violated the rule or is responsible for the violation.” *Id.* (c)(1). “Absent exceptional circumstances, a law firm must be held jointly responsible for a violation committed by its partner, associate, or employee.” *Id.* “A sanction imposed under [Rule 11] must be limited to what suffices to deter repetition of the conduct or comparable conduct by others similarly situated,” and “may include nonmonetary directives.” *Id.* (c)(4).

“Rule 11 . . . imposes an objective standard of reasonable inquiry which does not mandate a finding of bad faith.” *Chambers v. NASCO, Inc.*, 501 U.S. 32, 47 (1991). Rule 11 focuses on “the signer’s conduct” “at the time of filing.” *Jones v. Int’l Riding Helmets, Ltd.*, 49 F.3d 692, 695 (11th Cir. 1995) (emphasis and internal quotation marks omitted). “[T]he purpose of Rule 11 as a whole is to bring home to the individual signer his personal, nondelegable responsibility.” *Pavelic & LeFlore v. Marvel Ent. Grp.*, 493 U.S. 120, 126 (1989) (holding, prior to the 1993 amendment to Rule 11, that sanctions may be imposed on the individual attorney who signs the papers and not on the attorney’s law firm).

To impose Rule 11 sanctions *sua sponte*, the court must find that offending conduct is “akin to contempt.” *Kaplan v. DaimlerChrysler, A.G.*, 331 F.3d 1251, 1255 (11th Cir. 2003). This court does not understand that standard to require a

finding of subjective bad faith. Such a requirement would be inconsistent with explanations from the Supreme Court and the Eleventh Circuit that Rule 11 is objective, *see, e.g., Chambers*, 501 U.S. at 47; *Jones*, 49 F.3d at 695, and the reality that “[a]s originally drafted, Rule 11 set out a subjective standard, but the Advisory Committee determined that this standard was not working,” *Bus. Guides, Inc. v. Chromatic Commc’ns Enters., Inc.*, 498 U.S. 533, 549 (1991).

In 1993, Rule 11 was amended to provide that it “does not apply to . . . motions under Rules 26 through 37.” Fed. R. Civ. P. 11(d). The advisory committee’s note explains that:

Rules 26(g) and 37 establish certification standards and sanctions that apply to discovery disclosures, requests, responses, objections, and motions. It is appropriate that Rules 26 through 37, which are specially designed for the discovery process, govern such documents and conduct rather than the more general provisions of Rule 11. Subdivision (d) has been added to accomplish this result.

Fed. R. Civ. P. 11 advisory committee’s note 1993 amendment.

Local Rule 83.1(f) provides that attorneys may be disciplined for acts or omissions that are inconsistent with the local rules, the *Alabama Rules of Professional Conduct*, and the *American Bar Association Model Rules of Professional Conduct*. N.D. Ala. R. 83.1(f). It further provides that “[d]iscipline under this Rule may consist of disbarment, suspension, censure, reprimand, removal from a particular case, ineligibility for appointment as court-appointed counsel, ineligibility to appear under subsections (b) and (c), monetary sanctions, or any other

sanction the court may deem appropriate.” *Id.*

Alabama Rule of Professional Conduct 3.3 provides that “[a] lawyer shall not knowingly . . . [m]ake a false statement of material fact or law to a tribunal.” Ala. Rules of Pro. Conduct r. 3.3(a)(1). The comments to the Rule provide that “an assertion purporting to be on the lawyer’s own knowledge, as in an affidavit by the lawyer or in a statement in open court, may properly be made only when the lawyer knows the assertion is true or believes it to be true on the basis of a reasonably diligent inquiry.” Ala. Rules of Pro. Conduct r. 3.3. cmt. They further provide that “[l]egal argument based on a knowingly false representation of law constitutes dishonesty toward the tribunal. A lawyer is not required to make a disinterested exposition of the law, but must recognize the existence of pertinent legal authorities.” *Id.*

The sanction authority of the court is not limited to these rules. For more than two hundred years, “[i]t has long been understood that ‘[c]ertain implied powers must necessarily result to our Courts of justice from the nature of their institution,’ powers ‘which cannot be dispensed with in a Court, because they are necessary to the exercise of all others.’” *Chambers*, 501 U.S. at 43 (quoting *United States v. Hudson*, 7 Cranch 32, 34 (1812)).

“Courts have long recognized an inherent authority to suspend or disbar lawyers . . . derive[d] from the lawyer’s role as an officer of the court which granted

admission.” *In re Snyder*, 472 U.S. 634, 643 (1985). Thus, “a federal court has the power to control admission to its bar and to discipline attorneys who appear before it.” *Chambers*, 501 U.S. at 43 (citing *Ex parte Burr*, 22 U.S. 529, 530 (1824)). “An attorney who violates his or her ethical obligations is subject to professional discipline, including sanctions, suspension, and disbarment.” *Connick v. Thompson*, 563 U.S. 51, 66 (2011).

Although Rule 11 “reaches only certain individuals or conduct, the inherent power extends to a full range of litigation abuses.” *Chambers*, 501 U.S. at 46. “A court must . . . exercise caution in invoking its inherent power,” and “when there is bad-faith conduct in the course of litigation that could be adequately sanctioned under the Rules, the court ordinarily should rely on the Rules rather than the inherent power.” *Id.* at 50. “[I]f in the informed discretion of the court, neither the statute nor the Rules are up to the task, the court may safely rely on its inherent power.” *Id.*

“Because of their very potency, inherent powers must be exercised with restraint and discretion.” *Id.* at 44. “A primary aspect of that discretion is the ability to fashion an appropriate sanction for conduct which abuses the judicial process.” *Id.* at 44–45. The Supreme Court has held that even “particularly severe sanction[s]” are “within the court’s discretion.” *Id.* at 45 (discussing “outright dismissal of a lawsuit” as a sanction).

A finding of subjective bad faith or something tantamount to it is necessary to support a sanction issued pursuant to a court's inherent power. *See Purchasing Power, LLC v. Bluestem Brands, Inc.*, 851 F.3d 1218, 1223 (11th Cir. 2017). "A finding of bad faith is warranted where an attorney knowingly or recklessly raises a frivolous argument, or argues a meritorious claim for the purpose of harassing an opponent. A party also demonstrates bad faith by delaying or disrupting the litigation or hampering enforcement of a court order." *Barnes v. Dalton*, 158 F.3d 1212, 1214 (11th Cir. 1998) (quoting *Primus Auto. Fin. Servs., Inc. v. Batarse*, 115 F.3d 644, 649 (9th Cir. 1997)); accord *Thomas v. Tenneco Packaging Co.*, 293 F.3d 1306, 1320 (11th Cir. 2002).

"If particularly egregious, the pursuit of a claim without reasonable inquiry into the underlying facts can be the basis for a finding of bad faith." *Barnes*, 158 F.3d at 1214. "[I]n the absence of direct evidence of subjective bad faith, [the bad-faith] standard can be met if an attorney's conduct is so egregious that it could only be committed in bad faith." *Purchasing Power*, 851 F.3d at 1224–25; accord *Roadway Exp., Inc. v. Piper*, 447 U.S. 752, 767 (1980) (stating that inherent powers require a finding that "counsel's conduct . . . constituted or was tantamount to bad faith"). "This is not the same as simple recklessness, which can be a starting point but requires something more to constitute bad faith." *Purchasing Power*, 851 F.3d at 1225 (citing *Barnes*, 158 F.3d at 1214).

### **C. Findings and Conclusions as to Each Attorney and Butler Snow**

Because the motions at issue are discovery motions under Rules 30 and 37, Rule 11 “does not apply.” Fed. R. Civ. P. 11(d); Docs. 174, 182. This appears to be an unintended anomaly in Rule 11: the advisory committee’s note indicates that discovery motions were excepted from Rule 11 because the committee expected Rules 26 and 37 to allow courts to address sanctionable misconduct in such motions, but Rules 26 and 37 furnish no basis for the court to address the false statements of law these attorneys made in discovery motions. *See* Fed. R. Civ. P. 11 advisory committee’s note 1993 amendment; Fed. R. Civ. P. 26, 37. Regardless, Rule 11 says what it says, it does not apply here, and this court has no authority to change that.

Further, it is unclear to the court that Alabama Rule of Professional Conduct 3.3 applies to the misconduct at issue here. On the one hand, inserting into court filings unverified legal citations generated by AI is wholly inconsistent with the duty of candor that Rule 3.3 enumerates. On the other hand, by its terms Rule 3.3 forbids only knowing misstatements of law, and these false statements occurred because none of the three attorneys at issue bothered to verify the hallucinated citations (and two of them did not know that the citations had been generated by AI). As far as the court can discern, the Alabama Supreme Court has not yet had the opportunity to consider whether Rule 3.3 applies to this specific kind of misconduct. Absent such guidance, the court will not extend that rule beyond its plain terms.

Likewise, Local Rule 83.1(f) does not clearly forbid this misconduct. Rule 83.1(f) forbids (among other things) violations of the Alabama Rules of Professional Conduct in this federal district; it does not set out a separate and independent universe of forbidden conduct relevant here.

This series of gaps leaves the court with only its inherent authority. These are precisely the kind of gaps that the inherent authority must fill: although no specific rule expressly forbids the misconduct that occurred here, on the whole the rules make clear that it is serious misconduct ever to make false statements to a court, and no one here suggests that false statements generated by AI and parroted without verification in discovery motions are allowed. Indeed, Butler Snow appears to understand that it is a Rule 11 violation to sign a motion that parrots false statements generated by AI. *See* Doc. 195 at 5 (“Butler Snow does not dispute that it is within the Court’s discretion to sanction counsel’s conduct under Rule 11.”); Doc. 203 at 4 (Butler Snow, making arguments about appropriate sanctions under Rule 11 without discussing the exception for discovery motions).

The court thus assesses individually each lawyer’s conduct, as well as the firm’s, to determine whether it was bad faith or tantamount to it.

### **1. Lynette E. Potter**

Ms. Potter stated in her declaration that she “did not draft, edit, review, supervise, or approve the Motions or any drafts of the Motions,” and “possessed no

knowledge related to the preparation or filing of the Motions or any of their contents until May 16, 2025, when the Court entered its Show Cause Order.” Doc. 198-1 ¶ 5. Nothing in the record contradicts this account. Therefore, the court releases Ms. Potter from these disciplinary proceedings.

## **2. Daniel J. Chism**

Mr. Chism stated in his declaration that although he “was copied on emails circulating drafts,” he “did not draft, revise, or review the Motions [at issue].” Doc. 194-4 ¶ 4. Nothing in the record contradicts this account. Mr. Chism is an associate at Butler Snow without supervisory responsibility and no indication appears in the record that he delegated the use of his signature on these motions. Accordingly, the court releases Mr. Chism from these disciplinary proceedings.

## **3. Butler Snow**

Butler Snow proactively addressed the challenges of AI as early as June 2023, when all Butler Snow attorneys received an email from the firm’s general counsel warning them “that ‘there are significant risks that LLM [Large Language Model] output can appear perfectly researched and logical while in fact it is wholly inaccurate.’” Doc. 195-1 at 2–3, 6. In that same email, the firm announced a policy that requires “written permission from the appropriate Practice Group Leader to use this new technology as a secondary research tool, with full checks of the accuracy of any results through traditional legal research methods.” *Id.* at 6. (It was this very

policy that Mr. Reeves admitted he violated. *See* Doc. 194-2 ¶ 6.) At some point thereafter, the firm created an AI committee that made substantial progress on a more comprehensive firmwide AI policy. *See* Doc. 195-1 at 11–16. As these efforts were ongoing, individual Butler Snow attorneys (including Ms. Potter) wrote and published articles detailing the dangers associated with misuse of AI in legal work. Doc. 200 at 10–11.

After the court issued its show cause orders in this case, Butler Snow escalated its internal warning efforts. *First*, Mr. Watson “sent a reminder to all Butler Snow attorneys of their ethical and professional duties to verify the accuracy of all citations or other authority presented to any court.” Doc. 195-1 at 4, 17. *Second*, the firm “will conduct additional and extensive firm-wide training on the appropriate use of artificial intelligence, including training to ensure that any citation to authority, no matter its source, is accurate, truthful, and unquestionably stands for the proposition for which it is being offered.” *Id.* at 4. *Third*, the firm is updating its policies with lessons learned from this episode. For example, “Butler Snow will be adopting a prefiling protocol requiring (a) review of all legal authority in any document to be filed with a court of law and (b) confirming the existence, accuracy, and relevance of each citation.” *Id.* at 4–5. In addition, Butler Snow represented at the show cause hearing that it “need[s] to make clear” that junior attorneys who affix their signatures to a filing “must verify that” filing, even if a senior attorney sends it to them. Doc.

200 at 15–16.

Butler Snow understood the seriousness of these proceedings and responded accordingly. It called these events “unacceptable” and apologized in its initial response, Doc. 195 at 1, then it expressed similar contrition at every subsequent step. Acting on these sentiments, Butler Snow expended significant time and resources to investigate and remediate these issues through both an internal investigation of citations and a parallel investigation by Morgan Lewis. *See* Doc. 203 at 2. And at the show cause hearing, Butler Snow represented that Mr. Lunsford and Mr. Chism’s motion to be excused from the show cause hearing “should not have been filed,” and that the firm was unaware of the motion before it was filed. Doc. 200 at 13.

The court is well aware that the record may not reflect the fullness of Butler Snow’s internal response to the violation of firm policy. At the show cause hearing, when Mr. Lunsford described these disciplinary proceedings as “fresh and raw,” he explained that “the firm’s response to this is not complete yet.” Doc. 200 at 33.

In terms of legal arguments, “Butler Snow d[id] not dispute that it is within the Court’s discretion to sanction counsel’s conduct under Rule 11,” and acknowledged that “[a] law firm must be held jointly responsible for a violation committed by its partner, associate, or employee, absent exceptional circumstances.” Doc. 195 at 5 (citing Fed. R. Civ. P. 11(c)). Butler Snow has determined that “this was an isolated event” where “a single attorney failed to follow [firm] policies and

procedures and used unverified AI on the two filings in question.” Doc. 203 at 3–4.

Butler Snow also argues that the court should consider, among other things, the “magnitude of the harm” and the “significant publicity given to these events” to “limit any sanctions it may impose to a modest sanction upon [Butler Snow] and to the exclusion of the affected clients.” *Id.* at 5 (citing media reports). Butler Snow observes that “as shown by the corrected briefs, the legal propositions stated were not erroneous.” *Id.* at 4–5.

At the threshold, the court rejects the invitation to consider that actual authorities stand for the proposition that the bogus authorities were offered to support. That is a stroke of pure luck for these lawyers, and one that did not remediate the waste and harm their misconduct wrought. Further, any sanctions discount on this basis would amplify the siren call of unverified AI for lawyers who are already confident in their legal conclusion. This court will have no part of that.

Likewise, the court rejects the invitation to consider that the involved lawyers and firm have been deeply embarrassed in media reports. For many very good reasons, courts traditionally have not relied on the media to do the difficult work of professional discipline, and this court is not about to start.

When the court turns to the appropriate scope of its analysis as to Butler Snow — the firm’s own conduct — it finds that Butler Snow acted reasonably in its efforts to prevent this misconduct and doubled down on its precautionary and responsive

measures when its nightmare scenario unfolded. Accordingly, the court sees no evidentiary basis for a finding that the firm acted in bad faith or with such recklessness that its conduct was tantamount to bad faith. The court therefore releases the firm from disciplinary proceedings.

#### **4. Matthew B. Reeves**

Mr. Reeves admits that he utilized AI to generate the legal citations at issue, that he added them to both draft motions without verifying them, and that all of this was “contrary to the requirements of Butler Snow LLP and [his] obligations to this Court.” Doc. 194-2 ¶¶ 3–6. As the court understands Mr. Reeves’s position, he does not contest his responsibility in any way and would prefer to be held solely responsible. *See* Doc. 200 at 24. And the court credits Mr. Reeves’s representation that he will use his own experience in this case to warn law students and other lawyers of the consequences they might face if they make a similar decision regarding the use of AI. *See* Doc. 203-4 ¶¶ 3–5.

The court has no difficulty finding that Mr. Reeves’s misconduct was more than mere recklessness. In the light of repeated general warnings from federal courts about the risks of bogus citations generated by AI, as well as the persistent specific warnings, policies, and expectations of his colleagues and law firm with respect to AI, Mr. Reeves’s misconduct was particularly egregious. Having been so extensively alerted of the risk that AI will make things up, and having blown through

all of his firm's internal controls designed to protect court filings from counterfeit citations, Mr. Reeves's repeated decisions to parrot citations generated by AI without verifying even one of them reflect complete and utter disregard for his professional duty of candor. This is recklessness in the extreme, and it is tantamount to bad faith. Accordingly, the court will impose an appropriate sanction under its inherent authority.

### **5. William J. Cranford**

Mr. Cranford drafted, signed, and personally filed both motions at issue. Doc. 194-3 ¶¶ 4–19. He included the fabricated citations in these filings without reviewing any of them after Mr. Reeves inserted them. *Id.* ¶¶ 7, 17. Although Mr. Cranford did not know that Mr. Reeves used generative AI, Mr. Cranford had an obligation to check the citations before signing the motions and filing them with the court. Any reasonable investigation (indeed, even the most cursory of investigations, or a spot check) would have quickly revealed the problem. Mr. Cranford acknowledged his culpability at the show cause hearing: “I understand that by signing these motions, I was verifying and accepting responsibility for the contents of those motions. And I take full responsibility for that.” Doc. 200 at 18–19.

At the threshold, the court observes that if these motions had not been discovery motions, Mr. Cranford's conduct would have been a textbook Rule 11 violation. In any event, Mr. Cranford failed to discharge his most basic responsibility

as an attorney signing and filing motions with the court: to make sure that the statements in the motions were true. Mr. Cranford's repeated decisions to make no effort in this regard reflect a troubling indifference to the veracity of his court filings and disinterest in the most rudimentary demands of professional responsibility. This misconduct was more than simple recklessness and is particularly egregious, especially in the light of how little effort would have been required of Mr. Cranford to uncover any of the falsehoods. The unacceptable result of Mr. Cranford's decisions is that motions were filed with the court that no attorney ensured were free from false statements. Attorneys who sign motions must know — as Mr. Cranford acknowledges — that they risk serious sanctions when they make no effort to ensure that those motions tell the truth. Accordingly, the court finds that Mr. Cranford's misconduct was tantamount to bad faith and will sanction him under its inherent power.

To be clear, not every error in a motion is recklessness or more. To err is human, and minor typographical errors, even in citations, occasionally occur despite attorneys' best efforts. Likewise, some factual or legal authorities are the subject of reasonable debate, and a mere disagreement with one side's view does not necessarily mean that the view is objectively false. The insertion of bogus citations is not a mere typographical error, nor the subject of reasonable debate.

## 6. William R. Lunsford

Mr. Lunsford stated in his declaration that he did not review the motion for leave to depose and did review the motion to compel. Doc. 194-1 ¶¶ 9–10. Nevertheless, in accordance with his practice group’s ordinary workflow, Mr. Lunsford allowed Mr. Cranford to use his name in the signature block on both motions. *See id.* ¶¶ 9–11; *see generally* Doc. 200 at 25–26 (discussing how the “youngest lawyers primarily draft the documents”). As Mr. Lunsford stated in his declaration, his “name and signature appear on all of the current public contracts for professional services provided by outside legal counsel to the State of Alabama (the “State”) on a limited number of matters for which the State elects to hire outside counsel.” Doc. 194-1 ¶ 7. “As such, [he is] the principal responsible attorney for all matters currently assigned to [Butler Snow] regarding the Alabama Department of Corrections (“ADOC”).” *Id.* And as the Alabama Attorney General’s Office explained, Mr. Lunsford personally holds the designation of deputy attorney general; that designation allows him to represent Defendant Dunn and employ other attorneys in his firm (who do not have such a designation) to assist him. Doc. 200 at 39.

Mr. Lunsford did not know that Mr. Reeves utilized generative AI. Like Mr. Cranford, Mr. Lunsford simply made no effort whatsoever to verify the contents of the motions for himself (or even to ask someone else to check for him), despite his presence on these motions.

Outside of his hastily filed request to be excused from the show cause hearing, Mr. Lunsford has not argued that he is somehow not responsible for the false statements made to the court. *See* Doc. 194-1 ¶¶ 2, 6–7, 9–10, 13; *see also* Doc. 200 at 25–26. Indeed, when the firm explained its position that it understood it may be sanctioned, and he was offered the opportunity to explain how his position might differ from the firm’s, he accepted the firm’s position. Doc. 200 at 33.

Both before and at the show cause hearing, Mr. Lunsford deepened rather than allayed the court’s concerns about his understanding of his professional responsibility with respect to court filings that bear his name in the signature block.

*First*, Mr. Lunsford’s request to be excused from the show cause hearing reflected an intense lack of concern for the seriousness of the misconduct that both Plaintiff Johnson and the court had described. *See* Doc. 188. Either Mr. Lunsford personally reviewed the show cause order and decided to try to skip the hearing despite the accusation of fabricated citations, or he failed to personally review the order and made no effort to evaluate the seriousness of the issue before asking for a pass. Either way, Mr. Lunsford’s hasty excuse request troubled the court.

*Second*, after the court denied Mr. Lunsford’s request and before the hearing, Mr. Lunsford explained in his declaration his ordinary practices and his team’s workflow. *See* Doc. 194-1. He stated that this “this is the only instance in over a decade of working with Matt Reeves when [Mr. Lunsford] ha[s] ever encountered

an instance when [Mr. Reeves] added a citation that he failed to validate.” *Id.* ¶ 11. This is a big statement about ten years of work-product, but it came with no citation or other basis: Mr. Lunsford did not describe any workflow, nor any investigation, that would involve him actually evaluating, let alone ensuring, whether or how citations were validated, either in real time or historically. And other statements in his declaration undercut this hyperbole: he explained that as a rule, he simply assumes that other people verify citations. *See id.*

*Third*, at the hearing, when the court asked Mr. Lunsford about his use of AI, he explained that because the cases he handles as a deputy attorney general often involve similar facts and law, when the team he leads has a need for legal research in a case, it is their ordinary practice to re-use (apparently without verification) material from filings in other cases. *See* Doc. 200 at 27. This practice, Mr. Lunsford implied, obviated any need to rely on AI. *See id.* In any event, Mr. Lunsford made clear that performing (or verifying) legal research for each case is not something that he requires of the team he leads.

Mr. Lunsford’s statements at the hearing appear to the court to have deepened the concern at Butler Snow. Although the firm had conducted a preliminary investigation in the few days between the issuance of the show cause orders and the show cause hearing, it substantially broadened that investigation after the hearing, both investigating for itself and commissioning an independent investigation of

every filing (that contained citations) in every case “in all Alabama federal courts and the Eleventh Circuit Court of Appeals” where Mr. Lunsford, Mr. Cranford, Ms. Potter, Mr. Chism, or Mr. Reeves appeared on any filing since April 1, 2023. *See* Doc. 203 at 1–2. This was a very significant (and no doubt extremely expensive) undertaking.

On this factual record, the court has no difficulty finding that Mr. Lunsford bears responsibility for the false statements of law made to the court over his name in the signature block. He acknowledges as much and has apologized. *See* Doc. 194-1 ¶¶ 2, 6–7, 9, 13. Indeed, although Mr. Lunsford did not personally use AI to generate citations and did not personally file the motions at issue, the record does not suggest that he would have done anything differently than Mr. Cranford did, nor that he expected Mr. Cranford to do anything differently. According to Mr. Lunsford’s own testimony, he did not make any effort to verify the contents of the motion to compel before authorizing its filing, and it would have been extremely unusual for him to do so. Nor did he require (or even ask) Mr. Cranford or Mr. Reeves, or any other attorney (or person), to undertake that task. Nor was it his practice to require (or ask) that of them.

Like Mr. Cranford and Mr. Reeves, Mr. Lunsford simply assumed the truth of what was in the draft, and/or assumed that someone else would check on that. This is the same indifference to the truth and complete personal disinterest in the most

basic professional responsibility that Mr. Cranford displayed. Particularly in the light of Mr. Lunsford's roles as practice group leader, supervisory attorney, and partner — and the reality that he is the only lawyer on the team entrusted with the necessary deputy attorney general designation — this utter disregard for the truth of filings bearing his name in the signature block is particularly egregious, more than mere recklessness and tantamount to bad faith.

To be clear, the court's finding in this regard is not simply a harsh inference: when it became apparent that multiple motions with his name in the signature block contained fabricated citations, Mr. Lunsford's nearly immediate response was to try to skip the show cause hearing and leave the mess for someone else. And when the court compelled him to appear at the hearing, he paired his apology with an explanation in greater fullness of how very little work he personally puts in to be sure that his team's motions tell the truth. This cannot be how litigators, particularly seasoned ones, practice in federal court or run their teams. Accordingly, the court will impose an appropriate sanction under its inherent authority.

#### **D. Sanctions**

To exercise its inherent power with restraint and discretion, the court looks first to the purpose of that power. “The purpose of the inherent power is both to vindicate judicial authority without resorting to contempt of court sanctions and to make the non-violating party whole.” *Purchasing Power*, 851 F.3d at 1225 (citing

*Chambers*, 501 U.S. at 45–46). “This power is . . . for rectifying disobedience, regardless of whether such disobedience interfered with the conduct of the trial.” *Id.*

To rectify the bad-faith misconduct in this case and vindicate the lawful authority of federal courts to keep proceedings free from falsehoods, the court will impose the least severe sanction that the court finds likely to deter future similar misconduct. As the court exercises its inherent power in this factual context, it assigns primary value to the deterrent function of a sanction, for several reasons. *First*, this kind of AI misuse is a serious and time-sensitive problem that, unless it is arrested promptly, will impose escalating undue costs on litigants, cause extensive disruptions for courts, and damage public confidence in the legal community and the integrity of the justice system. At a minimum, protecting judicial authority requires effective preventive measures designed to reduce the practical likelihood that this kind of AI misuse continues apace.

*Second*, Rule 11 assigns particular value to the deterrent function of a sanction. *See* Fed. R. Civ. P. 11(c)(4) (providing that sanctions “must be limited to what suffices to deter repetition of the conduct or comparable conduct by others similarly situated”). Although Rule 11 does not control the court’s analysis because the motions at issue happen to be discovery motions, it is persuasive authority about the purpose that a sanction for false statements of law must serve.

And *third*, there is persuasive precedent in this Circuit for calibrating

sanctions issued pursuant to a court's inherent power to serve deterrence purposes. *See Boe v. Marshall*, 767 F. Supp. 3d 1226, 1295–97 (M.D. Ala. 2025) (imposing sanctions for bad-faith judge-shopping to serve deterrence purposes).

As the court considers an appropriate sanction, it also examines other cases involving false statements of law generated in the first instance by AI. In *Mata* and *Hayes*, which involved AI hallucinations that the lawyers first defended as real (before accepting responsibility), the district courts imposed modest monetary sanctions (ranging from \$1,500 to \$5,000) and notification requirements. *Mata*, 678 F. Supp. 3d at 449, 466; *Hayes*, 763 F. Supp. 3d at 1067, 1070, 1073.

Courts across the country have reacted similarly to other incidents involving misuse of artificial intelligence where the involved lawyers promptly accepted responsibility. *See, e.g., Versant Funding LLC v. Teras Breakbulk Ocean Navigation Enters., LLC*, No. 17-cv-81140, 2025 WL 1440351, at \*7 (S.D. Fla. May 20, 2025) (imposing monetary sanctions ranging from \$500 to \$1,000); *Ramirez v. Humala*, No. 24-cv-424-RPK-JAM, 2025 WL 1384161, at \*3 (E.D.N.Y. May 13, 2025) (imposing a \$1,000 monetary sanction); *Nguyen v. Savage Enters.*, No. 4:24-cv-00815-BSM, 2025 WL 679024, at \*1 (E.D. Ark. Mar. 3, 2025) (imposing a \$1,000 monetary sanction); *Wadsworth*, 348 F.R.D. at 499 (imposing monetary sanctions ranging from \$1,000 to \$3,000); *Gauthier*, 2024 WL 4882651 at \*3 (imposing a \$2,000 monetary sanction); *see also Lacey v. State Farm Gen. Ins. Co.*, No. 2:24-

cv-05205-FMO-MAA, 2025 WL 1363069, at \*5 (C.D. Cal. May 5, 2025) (ordering plaintiff's law firms to pay defendants \$31,100 in fees and costs).

And at least some of these courts have sanctioned law firms and/or lawyers who were unaware of the AI misuse in real time. *See, e.g., Wadsworth*, 348 F.R.D. at 493–94, 498–99 (sanctioning attorneys who “were not provided a copy of the [sanctionable] Motions to review prior to filing” and were not aware that artificial intelligence had been utilized but had delegated their signatures, reasoning that they “had a nondelegable duty to ensure a motion or filing is supported by existing law”); *Versant Funding LLC*, 2025 WL 1440351, at \*5–\*7 (imposing sanctions on local counsel for “filing a response without ensuring the accuracy of the case citation and principle of law” despite “t[aking] no part in” *pro hac vice* counsel’s drafting process utilizing AI).

Having considered these cases carefully, the court finds that a fine and public reprimand are insufficient here. If fines and public embarrassment were effective deterrents, there would not be so many cases to cite. And in any event, fines do not account for the extreme dereliction of professional responsibility that fabricating citations reflects, nor for the many harms it causes. In any event, a fine would not rectify the egregious misconduct in this case.

The court finds that (1) a public reprimand paired with a limited publication requirement, (2) disqualification, and (3) referral to applicable licensing authorities

are necessary to rectify the misconduct here and vindicate judicial authority. Disqualification fits well: lawyers should know that if they make false statements in court proceedings, they will no longer have the professional opportunity to participate in those proceedings. Similarly, litigants should have assurance that false statements will not be allowed in their cases, and no court should be required to allow an attorney responsible for making false statements in the proceedings to continue in the proceedings. Likewise, a public reprimand with limited publication fits: it makes other clients, counsel, and courts aware of the lawyer's misconduct so that they may assess whether any measures are needed to protect their proceedings. Finally, the referral to licensing authorities is a bare minimum in the light of the primary nature of a lawyer's professional responsibility not to make things up.

The court further finds that no lesser sanction will serve the necessary deterrent purpose, otherwise rectify this misconduct, or vindicate judicial authority. Mr. Cranford, Mr. Reeves, and Mr. Lunsford are well-trained, experienced attorneys who work at a large, high-functioning, well-regarded law firm. They benefitted from repeated warnings, internal controls, and firm policies about the dangers of AI misuse. They have regular access to gold-standard legal research databases. They must have known they would be deeply embarrassed in this kind of situation, and that there could be harsh consequences with the court and their law firm. And yet here we are. The reality that this lapse in judgment presented in the most

spectacularly unforced fashion underscores the need for more than a fine and reprimand.

The court further finds that any greater sanction would be excessive in the vindication of judicial authority. Butler Snow's internal review, as well as Morgan Lewis's independent investigation, reassure the court that suspension from the practice of law in the Northern District is not necessary to protect other courts or cases. And the court is mindful and appreciative that the involved lawyers are sincerely apologetic and remorseful, and that Mr. Reeves is committed to educating others about these matters as a preventive measure.

The court is well aware that disqualification "often work[s] substantial hardship on the client," *Norton v. Tallahassee Mem'l Hosp.*, 689 F.2d 938, 941 n.4 (11th Cir. 1982), but the court does not find hardship here. At the show cause hearing, the representative of the Alabama Attorney General did not suggest any hardship for Defendant Dunn. *See* Doc. 200 at 38–40. This makes sense: the Attorney General's Office has a ready team of capable attorneys who can step in to represent Defendant Dunn, some of whom already represent other defendants in this case. And even if there is some minor hardship, it must yield to the seriousness of the misconduct here. The case will remain stayed for thirty days for Defendant Dunn's new counsel to prepare to participate.

**E. Findings as to Defendant Dunn**

Defendant Dunn was unaware of his attorney's conduct before the court's order to show cause, so the court declines to sanction him.

**III. CONCLUSION**

The court **ORDERS** as follows:

1. The court **PUBLICLY REPRIMANDS** attorneys Matthew B. Reeves, William J. Cranford, and William R. Lunsford for their misconduct described in this order;

2. To effectuate their reprimand, Mr. Reeves, Mr. Cranford, and Mr. Lunsford are **ORDERED** to provide a copy of this order to their clients, opposing counsel, and presiding judge in every pending state or federal case in which they are counsel of record. They shall also provide a copy of this order to every attorney in their law firm. They must comply with this requirement within ten days from the date of this order and must certify to the court within twenty-four hours of that compliance that the requirement has been met;

3. To further effectuate the reprimands and deter similar misconduct by others, the Clerk of Court is **DIRECTED** to submit this order for publication in the Federal Supplement;

4. Mr. Reeves, Mr. Cranford, and Mr. Lunsford are **DISQUALIFIED** from further participation in this case;

5. Mr. Reeves, Mr. Cranford, and Mr. Lunsford are **DIRECTED** to provide the Clerk of Court with a listing of jurisdictions in which they are licensed to practice law within twenty-four hours of this order;

6. The Clerk of Court is **DIRECTED** to serve a copy of this order on the General Counsel of the Alabama State Bar and any other applicable licensing authorities for further proceedings as appropriate; and

7. Daniel J. Chism, Lynette E. Potter, and Butler Snow LLP are **RELEASED WITHOUT SANCTION** from these disciplinary proceedings.

**DONE** and **ORDERED** this 23rd day of July, 2025.



---

**ANNA M. MANASCO**  
UNITED STATES DISTRICT JUDGE

# FCA Suit Tainted By Expert's AI 'Hallucination' Gets Dismissed

By **Dan McKay**

Law360 (September 30, 2025, 3:53 PM EDT) -- A False Claims Act suit rocked by allegations of AI-generated hallucinations in an expert's report ended Tuesday after the federal government joined the case and quickly urged a Utah federal judge to throw it out.

In a one-page **order**, U.S. District Judge Tena Campbell granted the government's Monday **motion to intervene** and dismiss the case against a Salt Lake City-based anesthesiology practice, finding "good cause" to end the five-year lawsuit.

The motion wasn't opposed by the other parties in the case, she noted, including whistleblower Michael D. Khoury, a vascular surgeon.

Neither the judge's ruling nor the government's motion mention the falsehoods in an expert witness report that upended the case in July.

The "United States has determined that continued litigation of this qui tam action is not in the government's interests," the government said in its motion.

The dismissal comes after the Utah anesthesiologists in July flagged a series of **fabrications** in a medical billing expert's report, calling it an extraordinary example of artificial intelligence gone wrong.

The report relied on fake testimony from a government representative, false citations of government manuals, and made-up industry publications, the defendants said.

The doctors sought **sanctions** that would boot the relator and his counsel off the case.

Khoury told the court in August that he and his counsel were "**stunned**" to learn during a deposition that one of their experts had used generative AI to help draft his report. But they said withdrawing the report was an appropriate response, not kicking them off the case.

The litigation began in 2020 with Khoury's sealed complaint accusing Mountain West Anesthesia of improperly billing the government for anesthesia services.

Khoury said the defendants spent much of their time in the operating room engrossed in their smartphones and personal devices when they were supposed to be providing continuous anesthesia care.

The anesthesiologists in turn said the use of personal devices is common among medical professionals and has nothing to do with the government's payment decisions, citing testimony from the Centers for Medicare and Medicaid Services.

In Monday's motion, the government said it investigated the claims and opted against intervening in the case when it started.

However, it is empowered under the False Claims Act to join the case at a later date and seek dismissal if there is "good cause" to do so, the U.S. Department of Justice said.

The Supreme Court's 2023 decision in [Polansky v. Executive Health Resources](#)  makes clear that the government's views on why dismissal is warranted are entitled to substantial deference, it said.

Attorneys for Mountain West said they were pleased by the government's decision to end the case.

"More than two years ago, the defendants obtained testimony from CMS in this very case showing that the relator's allegations were meritless," Matthew M. Curley of Bass Berry & Sims PLC said in a statement Tuesday.

He added that recent events "only served to confirm our view that this case should not continue."

Scott D. Gallisdorfer of Bass Berry added that the defendants were shocked when they saw the contents of the relator's expert report.

"From our perspective, there was simply no credible explanation offered as to how something like that could have happened," he said. "Even as courts are increasingly dealing with AI-generated hallucinations, we have never seen anything like that."

The U.S. Attorney's Office for the District of Utah didn't respond Tuesday to a request for comment. The relator's counsel declined to comment.

The government is represented by Joel A. Ferre of the U.S. Attorney's Office for the District of Utah.

Khoury is represented by Brandon J. Mark and Hannah J. Ector of Parsons Behle & Latimer PC, Lynn M. Adam of Adam Law LLC, Robert A. Griffith of Robert A. Griffith Attorney at Law, and Tejinder Singh of Sparacino PLLC.

The Mountain West defendants are represented by Stephen T. Hester of Cohne Kinghorn PC, and Matthew M. Curley and Scott D. Gallisdorfer of Bass Berry & Sims PLC.

Dr. John E. Miner is represented by Rodney R. Parker and Richard Van Wagoner of Spencer Fane LLP.

The case is U.S. et al. v. Mountain West Anesthesia LLC et al., case number 2:20-cv-00372, in the U.S. District Court for the District of Utah.

--Additional reporting by Emily Sawicki and Dorothy Atkins. Editing by Adam LoBelia.



Neutral

As of: September 24, 2025 6:09 PM Z

## P.R. Soccer League NFP, Corp. v. Federación Puertorriqueña de Fútbol

United States District Court for the District of Puerto Rico

April 10, 2025, Decided; April 10, 2025, Filed

CIVIL NO. 23-1203 (RAM)

### Reporter

2025 U.S. Dist. LEXIS 69916 \*; 2025 LX 260302; 2025 WL 1080732

PUERTO RICO SOCCER LEAGUE NFP, CORP., et al., Plaintiffs, v. FEDERACIÓN PUERTORRIQUEÑA DE FUTBOL, et al., Defendants.

**Notice:** This decision contains references to invalid citations in the original text of the opinion. They are relevant to the decision and therefore have not been editorially corrected. Linking has been removed from those citations.

**Prior History:** [P.R. Soccer League NFP v. Futbol, 2024 U.S. Dist. LEXIS 8656, 2024 WL 149618 \(D.P.R., Jan. 12, 2024\)](#)

### Core Terms

---

quotation

**Counsel:** [\*1] For Puerto Rico Soccer League NFP, Corp., Juan M. Cornejo, Maria Larracuenta, Jose R. Olmo-Rodriguez, Joseph Marc Seralta-Ives, Futbol Boricua, Inc., Plaintiffs: Ibrahim Reyes, LEAD ATTORNEY, REYES LAWYERS, P.A., Coral Gables, FL; Jose R. Olmo-Rodriguez, Olmo & Rodriguez Matias Law Office, PSC.

For Ivan E. Rivera-Gutierrez, Federacion Puertorriquena de Futbol, Jose Martinez, Gabriel Ortiz, Luis Mozo-Canete, Defendants: Alexandra C. Casellas-Cabrera, LEAD ATTORNEY, Adsuar Muniz Goyco Seda & Perez-Ochoa, PSC, San Juan, PR; Andres Daniel Santiago-Lopez, LEAD ATTORNEY, Adsuar Muniz Goyco Seda & Perez-Ochoa, Puerto Rico, San Juan, PR; Edwin J. Seda-Fernandez, Eric Perez-Ochoa, LEAD ATTORNEYS, Adsuar Muniz Goyco Seda & Perez Ochoa PSC, San Juan, PR.

For Federation Internationale de Football Association, also known as, FIFA, Defendant: H. Christopher Boehning, LEAD ATTORNEY, PRO HAC VICE, Paul, Weiss, Rifkind, Wharton & Garrison LLP, New York, NY; Roberto A. Camara-Fuertes, LEAD ATTORNEY, Ferraiuoli, LLC, San Juan, PR; Suleicka Tulier-Vazquez, LEAD ATTORNEY, Ferraiuoli LLC, San Juan, PR.

For Confederation of North, Central America and Caribbean Association Football, also known as, CONCACAF, Defendant: [\*2] Anibal Alejandro Roman-Medina, LEAD ATTORNEY, O'Neill & Borges, LLC; Salvador J. Antonetti-Stutts, LEAD ATTORNEY, O'Neill & Borges, LLC, San Juan, PR; Amanda M. Blau, John Joseph Kuster, Jon Muenz, PRO HAC VICE, Sidley Austin LLP, New York, NY.

**Judges:** Raúl M. Arias-Marxuach, UNITED STATES DISTRICT JUDGE.

**Opinion by:** Raúl M. Arias-Marxuach

## Opinion

---

### OPINION & ORDER

RAÚL M. ARIAS-MARXUACH, United States District Judge

Pending before the Court is co-plaintiffs Puerto Rico Soccer League NFP, Corp.; Maria Larracuenta; Jose R. Olmo-Rodriguez; Joseph Marc Seralta-Ives; and Futbol Boricua, Inc.'s (collectively, "Plaintiffs") *Memorandum in Compliance* at Docket No. 190 in response to the Court's *Order to Show Cause* at Docket No. 187. For the reasons below, the Court concludes that Plaintiffs failed to show cause and sanctions are warranted.

### I. BACKGROUND

In response to various motions by Defendants<sup>1</sup>, Plaintiffs submitted four filings on March 9 and 13, 2025, namely: *Plaintiffs' Response in Opposition to Defendants' Joint Motion to Disqualify Plaintiffs' Counsel* (Docket No. 174); *Plaintiffs' Response in Opposition to Defendants' Joint Motion for Protective Order Limiting the Scope of Discovery* (Docket No. 175); *Plaintiffs' Response [\*3] in Opposition to Defendants' Joint Motion for Entry of a Protective and Confidentiality Order and Rule 502(d) Order* (Docket No. 176); and *Plaintiffs' Supplement to Response in Opposition to Defendants' Joint Motion for Entry of a Protective and Confidentiality Order and Rule 502(d) Order* (Docket No. 177) (collectively, the "*Motions*"). On March 17, 2025, Defendants filed a series of motions seeking leave to reply to Plaintiffs' filings at Docket Nos. 174, 175, and 176. (Docket Nos. 178; 179 and 180). In their arguments, Defendants claimed that Plaintiffs had made multiple citation errors and alleged that they had used generative artificial intelligence to write these motions. See *id.*

On March 18, 2025, this Court issued the *Order to Show Cause*, which was amended the following day. (Docket Nos. 181 and 187). The Court stated that the *Motions* contained "multiple citations that are incorrect, do not contain the quotes or content cited to, and reference cases that cannot be located and thus presumably do not exist." *Id.* The Court asked Plaintiffs to show cause "as to why sanctions should not be levied against them for violations" of Rules 1.1 and 3.3 of the Model Rules of Professional Conduct and of [Fed. R. Civ. P. 11\(b\)\(2\)](#). *Id.*

Plaintiffs filed their *Memorandum in Compliance* on March 21, [\*4] 2025. (Docket No. 190). Plaintiffs assert that they did not use artificial intelligence when drafting the *Motions*, but instead

---

<sup>1</sup>"Defendants" include Confederation of North, Central America and Caribbean Association Football, Federacion Puertorriquena de Futbol, Federation Internationale de Football Association, Jose Martinez, Luis Mozo-Canete, Gabriel Ortiz, and Ivan E. Rivera-Gutierrez.

committed various errors due to "human oversight under significant time constraints." *Id.* at 2. According to Plaintiffs, their citation errors were immaterial and inadvertent; no cases were fabricated, but instead, were misspelled, miscited, or misremembered during the drafting process. See *id.* at 3-13. Additionally, Plaintiffs argue that there is no evidence of artificial intelligence use as there are no "systematic fabrications" of errors. *Id.* at 14. Plaintiffs claim they have upheld their duty of candor to the Court under Model Rule 3.3, as their errors were unintentional and did not cause "actual prejudice." *Id.* at 15, 17-18. Plaintiffs assert that they have complied with Model Rule 1.1 as they have provided competent representation and their arguments are rooted in accurate and controlling caselaw, albeit with some citation errors. See *id.* at 16-17. They argue sanctions would be disproportionate given the lack of prejudice and bad faith as well as relatively minor nature of the errors. See *id.* at 15. Finally, Plaintiffs claim that their legal arguments were sufficiently [\*5] supported as to not violate the requirements of [Fed. R. Civ. P. 11\(b\)\(2\)](#). See *id.* at 18-19.

## II. APPLICABLE LAW

Federal court may levy sanctions under [Fed. R. Civ. P. 11](#), which "requires attorneys to take responsibility for the claims and defenses they represent" and make reasonable inquires to ensure that their representations to the courts are "well-grounded in both law and fact." [Cruz v. Savage, 896 F.2d 626, 630 \(1st Cir. 1990\)](#); [Fed. R. Civ. P. 11\(b\)](#). Arguments within a filing should be "warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law." [Fed. R. Civ. P. 11\(b\)\(2\)](#). Attorneys who violate [Rule 11\(b\)](#) may face sanctions after being given notice and a reasonable opportunity to respond. [Fed. R. Civ. P. 11\(c\)\(1\)](#); see also [Figueroa-Rodriguez v. Lopez-Rivera, 878 F.2d 1488, 1491 \(1st Cir. 1988\)](#) (citation omitted) ([Rule 11](#) incentivizes attorneys to act "in a manner bespeaking reasonable professionalism and consistent with the orderly functioning of the judicial system."). A court may initiate sanctions *sua sponte* or on motion. See [Fed. R. Civ. P. 11\(c\)\(2\)-\(3\)](#). Sanctions "must be limited to what suffices to deter repetition of the conduct or comparable conduct by others similarly situated." [Fed. R. Civ. P. 11\(c\)\(4\)](#). "[I]f imposed on motion and warranted for effective deterrence," sanctions can include "an order directing payment to the movant of part or all of the reasonable attorney's fees and other expenses [\*6] directly resulting from the violation." *Id.* Sanctions for violations of [Rule 11\(b\)\(2\)](#) are imposed against a party's counsel, not the party. See [Fed. R. Civ. P. 11\(c\)\(5\)\(A\)](#).

Federal courts also retain the inherent authority and discretion to manage their own affairs, including the levying of sanctions. See [Chambers v. NASCO, Inc., 501 U.S. 32, 43, 111 S. Ct. 2123, 115 L. Ed. 2d 27 \(1991\)](#). Appropriate sanctions may include assessing "attorney's fees against counsel." [Roadway Exp., Inc. v. Piper, 447 U.S. 752, 765, 100 S. Ct. 2455, 65 L. Ed. 2d 488 \(1980\)](#). This type of fee award "may go no further than to redress the wronged party for losses sustained; it may not impose an additional amount as punishment for the sanctioned party's misbehavior." [Goodyear Tire & Rubber Co. v. Haeger, 581 U.S. 101, 108, 137 S. Ct. 1178, 197 L. Ed. 2d 585 \(2017\)](#) (citation and internal question marks omitted). A properly calibrated fee award "covers the legal bills that the litigation abuse occasioned," requiring the sanctioning court "to establish a causal link" between the misbehavior and legal fees incurred by

the opposing party. *Id.* However, in cases where parties act "in complete bad faith," courts may shift more, if not all, of a party's fees. See *id.* at 110-11 (citing [Chambers, 501 U.S. at 51, 57-58](#)).

### III. DISCUSSION

The Court is not persuaded by Plaintiffs' arguments. As shown in the Appendix, Plaintiffs' filings were rife with citations for content that did not exist in the underlying opinion and quotations allegedly summarizing or restating the [\*7] case law, rather than the exact text of the opinion. The misuse of quotation marks was so prevalent that it was unusual for the Court to find a quotation provided by Plaintiffs within the case it was attributed to. Plaintiffs claim their actions are acceptable "minor paraphrasing" or "minor interpretive variances." (Docket No. 190 at 7, 9). The Court categorically rejects this assertion. When parties present quotations from other cases to the Court, they are indicating that the quoted content **actually exists** and that the Court can rely on their representations. If Plaintiffs wish to paraphrase content, they may do so without the use of quotation marks. Plaintiffs' refusal to recognize the problem with their "interpretive variances" is concerning. *Id.* at 9.

The Court could not find many of the proffered quotations or their equivalents within the cases they are attributed to. **On occasion, the text of a case relied on by Plaintiffs expressly contradicted or was unrelated to the content it was cited in support of.** Some cases were completely inapposite to the controversy at hand, so while Plaintiffs may have accurately paraphrased portions of an opinion, the opinion dealt with different [\*8] matters than those at issue in the *Motions*. For example, Plaintiffs quote [Poliquin v. Garden Way, Inc., 989 F.2d 527, 532 \(1st Cir. 1993\)](#) for the proposition that restricting counsel's access to discovery materials requires a "specific demonstration of need." (Docket No. 176 at 4). However, as noted at citation fifty in the Appendix, that case dealt with a different issue: whether and how material introduced at trial can be protected from disclosure afterwards. In no less than four instances, Plaintiffs say that discovery should be as broad as possible. Regardless of the cases cited, this is not the state of the law in 2025. Fed. R. Civ. P. 26(b)(1) states that discovery must be "relevant to any party's claim or defense and proportional to the needs of the case," a narrower standard than Plaintiffs erroneously and obstinately state.

Citations were incorrectly formatted with incorrect reporter numbers, attributed to the wrong circuits or districts, or provided incorrect party names. **Whether generative artificial intelligence was used or not is immaterial, what matters is that the Plaintiffs provided the Court with a litany of inaccurate information in support of their claims.** For example, Plaintiffs cite to [Sullivan v. Taglianetti, 588 F.2d 1355, 1357 \(1st Cir. 1978\)](#); [United States v. Gannett Co., 835 F.2d 392, 395 \(1st Cir. 1987\)](#); and [Healey v. Gonzalez, 747 F.3d 111, 121 \(1st Cir. 2014\)](#). (Docket Nos. 175 and 176). As discussed in the Appendix, [\*9] none of these cases exist as cited. The Court could not locate [Sullivan v. Taglianetti](#). Similarly, while the Court has found two antitrust cases from the District of Columbia with similar citations to [United States v. Gannett Co.](#), their contents do not align with Plaintiffs' representations. The same is true for [Healey v. Gonzalez](#); while Plaintiffs identify the case they meant to cite to, that case has nothing to do with the propositions Plaintiffs cite it in support of. These are hardly minor errors.

The Court cannot agree with Plaintiffs that these errors do not violate the Model Rules or [Fed. R. Civ. P. 11\(b\)\(2\)](#). Model Rule 1.1 requires a lawyer to provide "competent representation" to clients, which requires the "legal knowledge, skill, thoroughness, and preparation reasonably necessary" for representations. Model Rules of Pro. Conduct R. 1.1 (Am. Bar Ass'n). Plaintiffs' counsel cannot be said to have behaved with the requisite "thoroughness and preparation" given their admitted haste in drafting the *Motions* and dozens of errors that resulted. If, indeed, Plaintiffs' errors were not made knowingly, they did not violate Model Rule 3.3, but the breadth of their errors remains striking. Model Rules of Pro. Conduct R. 1.1 (Am. Bar Ass'n). Plaintiffs claim that their counsel was facing tight deadlines, but Plaintiffs could have requested an extension to file [\*10] the *Motions* and, in any event, submitted these filings well before the deadline imposed by the Court. (Docket Nos. 164; 168 and 169).

Sanctions are appropriate given the extent of the errors in the *Motions* and the subsequent time and energy required by Defendants and the Court to fact-check Plaintiffs' filings. [Rule 11\(b\)\(2\)](#) provides additional grounds for sanctions as Plaintiffs' counsel cannot plausibly be understood to have made reasonable inquiries to ensure their representations are "well-grounded in both law and fact." [Cruz, 896 F.2d at 630](#). A simple Google search would have shown the problems in some of Plaintiffs' citations. In other instances, a quick search of the opinion Plaintiffs cited to would have revealed problems. Levying appropriate sanctions here promotes deterrence without being overly punitive, as contemplated by [Rule 11\(c\)\(4\)](#).

The Court notes that, rather than showing contrition, the *Memorandum in Compliance* strikes a defiant and deflective tone. (Docket No. 190). It also contains more of the errors that plagued Plaintiffs' previous four filings. For example, in the "Legal Standard" section of the memorandum, Plaintiffs cite to two cases for the proposition that sanctions are an "extreme remedy" appropriate [\*11] for instances of prejudice or bad faith. One case makes no mention of sanctions and neither contain the proffered quote *Id.* at 3. The Court finds it problematic that Plaintiffs responded to a show cause order to address the problem of multiple inaccurate citations by providing a response containing more erroneous citations.

Given the amount of problematic content in the *Motions* and time required by both Defendants and the Court to address them, the Court concludes that sanctions are appropriate under [Rule 11](#) and the Court's inherent authority. See [Chambers, 501 U.S. at 43](#) (noting that federal courts have the inherent ability to issue sanctions). Plaintiffs' counsels are therefore **ORDERED** to pay the attorneys' fees incurred by Defendants in relation to Plaintiffs' filings at Docket Nos. 174, 175, 176, and 177. Defendants are granted twenty-one days to submit an itemized application for attorney's fees. The Court warns Plaintiffs that if further problems of this nature or gravity happen again, it will move to revoke Mr. Ibrahim Reyes' *pro hac vice* status and refer any implicated attorneys for disciplinary proceedings.

**IT IS SO ORDERED.**

In San Juan, Puerto Rico, this 10th day of April 2025.

/s/ Raúl M. Arias-Marxuach

UNITED [\*12] STATES DISTRICT JUDGE

<i>Plaintiffs' Response in Opposition to Defendants' Joint Motion to Disqualify Plaintiffs' Counsel</i> (Docket No. 174)		
Citation:	Location:	Issue:
1. <u>Fiandaca v. Cunningham</u> , 827 F.2d 825, 829 (1st Cir. 1987).	Pg. 3, ¶ 2	<p>Plaintiffs quote this case for the proposition that the First Circuit requires "specific instances" of conflict, not "hypothetical scenarios" to warrant an attorney's disqualification.</p> <p>These quotes are not in the opinion, and the opinion does not support the proposition this case is cited for. On page 831, <u>Fiandaca</u> rejects a party's argument that has "simply no evidence" to support it. However, rejecting an argument that provides no evidence in support of its assertions is different than requiring "specific instances" of conflict. The opinion does not provide further statements in support of Plaintiffs' assertion here.</p>
2. <u>Id.</u>	Pg. 5, ¶ 1	<p>Plaintiffs quote <u>Fiandaca</u> to argue that the First Circuit applies Model Rule 3.7 "narrowly" to avoid "tactical misuse."</p> <p>These quotes are not in the opinion and the proposition this case is cited for is not supported by language in the opinion. Page 831 contains somewhat similar language: "disqualification motions can be tactical in nature." However, <u>Fiandaca</u> does not mention Model Rule 3.7, and as discussed previously, it only holds that a party's motivation in bringing motions to disqualify are "not irrelevant" because "disqualification motions can be</p>

		tactical in nature, designed to harass opposing counsel."
3. <u>Id.</u> at 829.	Pg. 6, ¶ 1	<p>Plaintiffs quote this case to state that Defendants' Rule 1.7 claim is "wholly speculative" because they "provide no evidence of [Mr. Reyes having] an ongoing financial stake or divergence from co-plaintiffs' goals."</p> <p>This quote is not in the opinion. While the Court does not take issue with the content of Plaintiffs' assertion, the Court finds no language in the opinion to support Plaintiffs' argument here. Citing <u>Fiandaca</u> for this proposition is thus incorrect.</p>
4. <u>Id.</u> at 830.	Pg. 6, ¶ 2	<p>The parenthetical to this citation states that early disqualification is "unduly punitive" without evidence. This quote is not in the opinion. Plaintiffs use the citation to support their claim that the First Circuit's purported preference for delay over preemptive action is controlling.</p> <p>That is not supported by the text of the opinion, as the First Circuit only held that otherwise valid motions for disqualification should not be ignored to save time. As explained at pages 830-31 of <u>Fiandaca</u>, the lower court had recognized a "probable existence of conflict" by plaintiffs' counsel, but denied a motion to disqualify on grounds of "necessity" to avoid further delays and proceed to trial. The First Circuit reversed, finding that "absent some evidence of true necessity, we will not permit a meritorious</p>

		disqualification motion to be denied in the interest of expediency unless it can be shown that the movant strategically sought disqualification in an effort to advance some improper purpose.”
5. <u>Id.</u>	Pg. 7, ¶ 3	<p>Plaintiffs cite to this case for the assertion that disqualification would unduly prejudice Plaintiffs.</p> <p>The proposition is not supported by the opinion because the issue in <u>Fiandaca</u> was that the denial of a meritorious motion for disqualification left the moving party at “significant risk of being prejudiced” by the outcome of the litigation. Here, Plaintiffs are seeking to prevent disqualification, not obtain it.</p>
6. <u>Kevlik v. Goldstein</u> , 724 F.2d 844, 850 (1st Cir. 1987).	Pg. 2, ¶ 1	<p>Plaintiffs cite this case to claim that the First Circuit demands a “high standard” for disqualification.</p> <p>This quote is not in the opinion, and the proposition this case is cited for is not supported by the language in the opinion. This case does involve disqualification and pages 850-51 discuss the “substantially related” test for “disqualification cases involving a conflict of interest based on the actual or potential threat of the violation of the attorney-client privilege.” However, the Court finds no equivalent wording describing the standard for disqualification as a high one.</p>
7. <u>Id.</u>	Pg. 2, ¶ 2	Plaintiffs cite this case to claim a party’s choice of counsel is a “valued right,” particularly in civil cases, and courts must

		<p>balance it against ethical concerns with “scrupulous care.”</p> <p>These quotes are not in the opinion and the proposition this case is cited for is not fully supported by the language in the opinion. While the Court does not dispute that a party’s choice to counsel is valuable, page 848 of the opinion clearly states that unlike criminal cases, civil cases lack the “rigorous sixth amendment protection of the right to the choice of counsel....We think it more important that unethical conduct be prevented than that defendant have an unfettered right to counsel of its choice.” The second-to-last paragraph of page 850 makes a similar point— that parties in civil actions have less protection in terms of their choice of counsel.</p>
<p>8. <u>Id.</u></p>	<p>Pg. 4, ¶ 1</p>	<p>Plaintiffs quote this case in a parenthetical finding that disqualification of counsel is unwarranted without “demonstrable detriment.”</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. The “substantially related” test for disqualification of counsel used on pages 850-51 does not support Plaintiffs’ claim that “demonstrable detriment” is needed for disqualification. Instead, the test states that a “former client need show no more than that the matters embraced within the pending suit wherein his former attorney appears on behalf of his adversary are</p>

		substantially related to the matters or cause of action wherein the attorney previously represented" the former client now seeking disqualification. Courts "will assume" that during the first representation, the former attorney received confidential information, but "will not inquire into their nature and extent." This implicitly recognizes that both actual and potential threats of violation of attorney-client privilege can cause disqualification.
9. <u>Id.</u>	Pg. 5, ¶ 4	<p>Plaintiffs use this quote to argue that the First Circuit requires a "specific showing" of conflicting interests, not mere affiliation when determining whether an attorney is conflicted under Model Rule 1.7.</p> <p>The quote is not in the opinion and the proposition this case is cited for is not fully supported by language in the opinion. As discussed above, <u>Kevlik</u> applied the "substantially related" test at pages 850-51. Courts applying this test can "assume that during the course of the former representation confidences were disclosed to the attorney bearing on the subject matter of the representation" and "will not inquire into their nature and extent." This implicitly rebukes Plaintiffs' assertion that specific evidence of conflicting interests is required for an attorney to be disqualified.</p>
10. <u>Id.</u> at 851.	Pg. 7, ¶ 1	Plaintiffs quote this case to argue that Model Rule 3.7(a)(3) exempts counsel from disqualification if it causes

		<p>substantial hardship, which the First Circuit interprets broadly to protect clients from “unnecessary disruption.”</p> <p>The quote and proposition this case is cited for is not supported by language in the opinion. Despite attributing this to <u>Kevlik</u>, the Court finds no mention of Model Rule 3.7 or its “substantial hardship” provision. Model Rule 3.7 relates to ethical issues arising out of a lawyer serving as an advocate at a trial they are likely to be a witness at, but in this case, the counsel for which disqualification was sought was not testifying at trial. Instead, this case dealt with a conflict between a lawyer’s current and former clients. Furthermore, footnote 4 of this case explicitly acknowledges that the Model Rules of Professional Conduct were not the controlling reference in <u>Kevlik</u>. The earlier Model Code of Professional Responsibility was used because it was in effect at the time of the disqualification motion. Although either set of rules would have resulted in the same result, the Model Rules did not govern resolution of this issue.</p>
<p>11. <u>Id.</u> at 850.</p>	<p>Pg. 7, ¶ 3</p>	<p>Plaintiffs cite this case for the proposition that no “clear and convincing” Model Rule 1.7 conflict exists.</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. As stated above, the Model Rules of Professional Conduct were not the</p>

		controlling authority in <u>Kevlik</u> . There is also no mention of Model Rule 1.7 in the opinion. <u>Kevlik</u> provides no support for this assertion.
12. <u>Culebra Enters. Corp. v. Rivera-Rios</u> , 846 F.2d 94, 97 (1st Cir. 1988).	Pg. 2, ¶ 2	<p>Plaintiffs quote this case to argue that the First Circuit views disqualification as an "extreme sanction" that "should be employed only after careful consideration."</p> <p>The quotes are not in this case and the proposition this case is cited for is not supported by language in the opinion. The opinion does not use language similar to that quoted by Plaintiffs, nor did it make findings on disqualification of counsel. Instead, <u>Culebra Enters. Corp.</u> dealt with the issues of whether it was proper to sanction attorneys, who expected to testify at trial but still provided pretrial legal work for the plaintiffs, by preventing them from recovering legal fees for their work. It also briefly discussed the ethical standard that should apply when determining whether the attorneys' behavior was ethical.</p>
13. <u>Id.</u> at 99.	Pg. 4, ¶ 1	<p>Plaintiffs quote this case to say that informed consent cures Model Rule 1.7 conflicts and that ethical rules are "flexible" when there is no systematic harm.</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. While a client's informed consent is required for a lawyer with a concurrent conflict to continue the representation, the text of</p>

		<p>Model Rule 1.7(b)(1)-(4) establishes there are three other criteria that must be satisfied for the conflict to be cured. Informed consent cannot unilaterally cure a conflict. Additionally, the Court finds nothing in the opinion discussing Model Rule 1.7 or supporting Plaintiffs' claim that ethical rules can be construed flexibly in the absence of systematic harm. As stated above, <u>Culebra Enters. Corp.</u> focused on resolving whether attorneys who expected to testify at trial could recover fees for their pretrial legal work on the same matter. The attorneys had faced sanctions for their purportedly unethical conduct and had lost the challenged fees as a result.</p>
<p>14. <u>Id.</u> at 99-100.</p>	<p>Pg. 4, ¶ 2</p>	<p>Plaintiffs state that the <u>Culebra Enters. Corp.</u> court held that a lawyer-witness may continue pretrial representation, with disqualification deferred until "actual necessity" is shown.</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. However, the opinion made narrower findings, observing that Model Rule 3.7 "is limited to situations where the lawyer-witness acts as trial counsel" at page 99, and noting that ethical concerns of retaining a lawyer-witness are ameliorated "when the lawyer-witness does not act as trial counsel, even if he performs behind-the-scenes work for the client in the same case." The court went no further than determining that a lawyer could</p>

		be both called as a witness and work on pretrial legal matters for the same case. The Court sees no language requiring that disqualification be deferred until actual necessity of the lawyer serving as a witness is determined.
15. <u>Id.</u> at 100.	Pg. 4, ¶ 2	<p>Plaintiffs say that the necessity of Mr. Olmo's testimony is untested and, in a parenthetical, state necessity is assessed "in light of available alternatives."</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by the opinion. The Court finds no language that supports this assertion, discusses the need for available alternatives, or establishes a broader benchmark for "necessity."</p>
16. <u>Id.</u> at 99.	Pg. 6, ¶ 1	<p>Plaintiffs quote this case in a parenthetical stating that ethical rules prioritize "practical outcomes" over rigid bans.</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. The court's actual finding on page 99 was narrower, stating that under Model Rule 3.7, "the prohibition against acting as 'advocate at a trial'" should not be read as "broadly prohibiting the rendition of case-related out-of-court services prior to trial." <u>Culebras Enters. Corp.</u> did not make a broader finding that ethical rules prioritize practicality over formality, nor does it support such an assertion.</p>

17. <u>Id.</u> at 100.	Pg. 6, ¶ 2	<p>Plaintiffs quote this case to claim that the First Circuit requires “actual necessity” for Model Rule 3.7 disqualification, not “potential relevance.”</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. Plaintiffs presumably mean that the First Circuit requires counsel to be a necessary witness in a proceeding (not a potential witness who may be relevant) before they can be disqualified under Model Rule 3.7. However, the Court does not find support for this argument in the opinion. <u>Culebras Enters. Corp.</u> did not address disqualification of counsel either, as the attorneys in question had not been disqualified (only subject to financial sanctions in the form of lost fees). The opinion does include the text of Model Rule 3.7 in a footnote but does not discuss the interplay between “necessity” and disqualification under Model Rule 3.7 as represented by Plaintiffs.</p>
18. <u>Id.</u>	Pg. 6, ¶ 2	<p>Plaintiffs use this case to say that disqualification of counsel is deferred until the necessity of the counsel to testify as a witness is “clearly established.”</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. As discussed above, disqualification was not the issue in this case (which dealt with sanctions), and the Court finds nothing in the</p>

		opinion that supports this assertion.
19. <u>Id.</u>	Pg. 7, ¶ 1	<p>Plaintiffs cite to this case with a parenthetical stating that hardship weighs heavily against disqualification.</p> <p>This case cites to and discusses Model Rule 3.7, which holds that a lawyer cannot be an “advocate at a trial in which the lawyer is likely to be a necessary witness except where,” <i>inter alia</i>, the disqualification of the lawyer would cause “substantial hardship on the client.” However, Plaintiffs’ citation is not supported by the text of the opinion, which does not specifically hold that hardship weighs “heavily” against disqualification.</p>
20. <u>Id.</u> at 99.	Pg. 7, ¶ 3	<p>Plaintiffs cite to this case for the proposition that applying Model Rule 3.7 to their counsel now is premature.</p> <p>While Model Rule 3.7 is cited to in the opinion, the opinion does not determine when it is likely that a lawyer will be a necessary witness in a trial. Plaintiffs’ proposition is not supported by the text of the opinion.</p>
21. <u>Estrada v. Cabrera</u> , 632 F.Supp. 1174 (D.P.R. 1986).	Pg. 2, ¶ 2	<p><b><u>The case does not exist as cited.</u></b></p> <p>Plaintiffs cite to <u>Estrada v. Cabrera</u>, 632 F.2d 1007, 1012 (1st Cir. 1980). The correct citation is presumably <u>Estrada v. Cabrera</u>, 632 F.Supp. 1174 (D.P.R. 1986), which is not a First Circuit case.</p> <p>Plaintiffs’ citation quotes this case for the proposition that disqualification of a party’s counsel is “not lightly granted,”</p>

		but this quote is not in the opinion. Similar wording is found on page 1175. For example, <u>Estrada</u> states: "the rule of disqualification should not be mechanically applied," and "[t]o disqualify a party's chosen attorney is a serious matter which could not be supported by the mere possibility of a conflict."
22. <u>Id.</u>	Pg. 3, ¶ 2	<p>Plaintiffs state that the <u>Estrada</u> court upheld counsel's representation despite alleged conflicts, finding no "actual showing" of divided loyalty.</p> <p>The quote is not in the opinion, but similar wording is found on page 1177. For example, <u>Estrada</u> states: "Under the facts of this case we find that there is no basis for the disqualification of the law firm." However, the proposition this case is cited for is not supported by language in the opinion because the alleged violation in <u>Estrada</u> was evaluated under Rules 1.6, 1.9 and 1.16 of the Canons of the American Bar Association, not the Model Rules of Professional Conduct.</p>
23. <u>Id.</u>	Pg. 5, ¶ 2	<p>Plaintiffs use this case in a parenthetical stating disqualification requires "tangible harm," not "theoretical risks."</p> <p>The quotes are not in the opinion and the proposition this case is cited for is contradicted by language in the opinion. On page 1176, the court states "[t]he relevant test in disqualification cases premised on those grounds [at stake in <u>Estrada</u>] and</p>

		<p>involving a conflict of interest based on the actual or potential threat of the violation of the attorney-client privilege is the 'substantially related' test." The recognition of a "potential" threat undercuts Plaintiffs' assertion that "theoretical risks" could not give rise to disqualification of counsel. There was no support elsewhere in the opinion for Plaintiffs' assertion.</p>
24. <u>Id.</u>	Pg. 7, ¶ 2	<p>Plaintiffs use this case to argue that delays in filing motions to disqualify signals bad faith and claim that late motions to disqualify are "viewed skeptically."</p> <p>The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. While page 1175 acknowledges that motions to disqualify should be approached with "cautious scrutiny" and can be used "for purely strategic purposes," there is no language in the opinion indicating that a party's decision to file a motion to disqualify later on in legal proceedings should be viewed with greater scrutiny than similar motions filed earlier. There is no support for the assertion that delays in filing motions to disqualify "signal bad faith," as represented by Plaintiffs.</p>
25. <u>Polyagro Plastics, Inc. v. Cincinnati Milacron, Inc.</u> , 903 F.Supp. 253,	Pg. 2, ¶ 2	<p>Plaintiffs quote to this case to say that parties moving for disqualification under the Model Rules of Professional Conduct must show a "clear and convincing" violation that threatens judicial integrity.</p>

256 (D.P.R. 1995).		The quote is not in the opinion and the proposition this case is cited for is not supported by language in the opinion. Page 256 recognizes "the protection of the integrity of the judicial process" as one of two competing interests when deciding a motion to disqualify. However, the Court found no language about the standard for a movant's burden of proof in a motion to disqualify that mirrors the "clear and convincing" requirement provided by Plaintiffs.
26. <u>In re Grand Jury Proceedings</u> , 859 F.2d 1021, 1026 (1st Cir. 1988).	Pg. 2, ¶ 2	Plaintiffs attribute quotes to this case to assert that a party seeking to disqualify counsel must show "actual prejudice" instead of "mere possibility."  These quotes are not in the opinion. Similar wording is found on page 1026, but it does not support Plaintiffs' proposition. The First Circuit states that they did not find "an actual, or even a serious potential for conflict of interest" in the record, noting that while "the district court stated that it had found an actual conflict of interest, it did not identify any specific conflict, actual or potential." While the court would not rely on "tenuous inferential relationships" to affirm the district court's order, the language in the opinion still indicates that a potential conflict of interest could suffice for disqualification, provided it is specific enough. Furthermore, pages 1023 and 1024 quote <u>Wheat v. United States</u> , 486 U.S. 153 (1988) for the

		proposition that trial courts can disqualify counsel because of potential conflicts.
27. <u>Id.</u>	Pg. 4, ¶ 1	<p>Plaintiffs quote this case to say that the First Circuit does not let parties "second-guess" opposing co-parties' decision to retain joint counsel unless there is clear abuse.</p> <p>The quote is not in the opinion. The proposition this case is cited for is contradicted by language in the opinion. In <u>In re Grand Jury Proceedings</u>, the Government challenged the decision of a defendant and immunized witness to have the same lawyer, without presenting evidence of clear abuse. The district court let the challenge proceed, and although the First Circuit was not convinced the Government met its burden to prove disqualification, the Government was able to "second-guess" the parties' choice of joint counsel.</p>
28. <u>Id.</u>	Pg. 5, ¶ 2	<p>Plaintiffs quote this case as showing that the First Circuit dismisses privilege gamesmanship concerns (here, Defendants' concerns that Mr. Olmo's dual plaintiff-counsel status could create an unfair advantage in litigation) absent "actual prejudice."</p> <p>The quote is not in the opinion and the proposition this case is cited for is contradicted by language in the opinion. Despite Plaintiffs' representations, in this opinion, the First Circuit does not require "actual prejudice" to disqualify a party's attorney. Instead, page</p>

		1024 states that "a showing of a serious potential for conflict" may lead to disqualification and page 1026 indicates that a "serious potential for conflict of interest" could be grounds for disqualification.
29. <u>Id.</u> at 1025.	Pg. 5, ¶ 2	<p>Plaintiffs' parenthetical for this case states that privilege issues are resolved on a "case-by-case" basis, not preemptively.</p> <p>This quote is not in the opinion. Similar wording is found on page 1024, which quotes <u>Wheat</u>, 486 U.S. at 163: ""The evaluation of the facts and circumstances of each case...must be left primarily to the informed judgment of the trial court." The First Circuit then noted that although <u>Wheat</u> was a criminal case that dealt with a Sixth Amendment issue, the standards may also apply to the grand jury context (as this case involved), at least in part.</p>
30. <u>Id.</u>	Pg. 6, ¶ 3	<p>Plaintiffs cite this case to say the First Circuit requires "intentional deceit" for Model Rule 8.4 violations.</p> <p>However, this quote is not in the opinion and the proposition is contradicted by the language of the opinion, which makes no mention of Model Rule 8.4, which covers attorney misconduct. The opinion briefly mentions the Model Code of Professional Responsibility— not the Model Rules of Professional Conduct— and in the context of an attorney's duty of loyalty to a client and duty not to disclose to another confidential information received from a</p>

		client. The issue of attorney misconduct is not addressed.
31. <u>Herrera-Venegas v. Sanchez-Rivera</u> , 681 F.2d 41, 42 (1st Cir. 1982).	Pg. 3, ¶ 3	<p>Plaintiffs quote this case to assert that the First Circuit recognizes 28 U.S.C. § 1654 as protecting a “fundamental” right to self-representation and, in an accompanying parenthetical, quotes <u>Herrera-Venegas</u> as stating § 1654 ensures litigants “may conduct their own cases.”</p> <p>These quotes are not in the opinion, and the opinion does not support the proposition Plaintiffs use it in support of. The opinion cites § 1654 for the proposition that “[b]y law, an individual may appear in federal courts only pro se or through legal counsel.” However, in <u>Herrera-Venegas</u>, the First Circuit held that a prisoner could not obtain third-party lay representation; § 1654 was used to show that an individual could only appeal in federal court via: (i) pro se litigants or (ii) legal counsel. The decision did not single out self-representation as a fundamental right.</p>

<i>Plaintiffs’ Response in Opposition to Defendants’ Joint Motion for Protective Order Limiting the Scope of Discovery</i> (Docket No. 175)		
Citation:	Location:	Issue:
32. <u>Oppenheimer Fund, Inc. v. Sanders</u> , 437 U.S. 340, 351 (1978).	Pg. 2, ¶ 2	Plaintiffs quote this case for the proposition that Fed. R. Civ. P. 26(b)(1) “casts a wide net” for discovery and lets parties pursue discovery that “bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case.”

		<p>These quotes are not in the opinion. However, page 351 discusses the boundaries of discovery under Rule 26(b)(1), stating in part that the rule "has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." Be that as it may, as of 2025, discovery is subject to a relevance and proportionality requirement. Fed. R. Civ. P. 26(b)(1).</p>
<p>33. <u>In re New England Compounding Pharm., Inc. Prods. Liab. Litig.</u>, No. 13-2419, 2013 WL 6058483 (D.Mass. Nov. 13, 2013).</p>	<p>Pg. 2, ¶ 2</p>	<p><b><u>The case does not exist as cited.</u></b> Plaintiffs cite to <u>In re New England Compounding Pharm., Inc. Prods. Liab. Litig.</u>, 752 F.3d 49, 54 (1st Cir. 2014). The right case is presumably <u>In re New England Compounding Pharm., Inc. Prods. Liab. Litig.</u>, No. 13-2419, 2013 WL 6058483 (D.Mass. Nov. 13, 2013).</p> <p>This case is quoted as stating Fed. R. Civ. P. 26 has a "broad sweep." This quote is not in the opinion, but page *3 makes multiple statements of this nature, such as noting that "Rule 26(b)(1) generally permits liberal discovery of relevant information."</p>
<p>34. <u>Id.</u> at 54.</p>	<p>Pg. 4, ¶ 1</p>	<p>Plaintiffs quote this case to state that Defendants' allegedly exclusionary conduct are "inextricably intertwined" with the alleged antitrust conspiracy, and thus discoverable.</p> <p>This quote is not in the opinion, however, there is some support for Plaintiffs' assertions on page *3, which states: "As the</p>

		Supreme Court has instructed, because 'discovery itself is designed to help define and clarify the issues,' the limits set forth in Rule 26 must be 'construed broadly to encompass any matter that bears on, or that reasonably could lead to other matters that could bear on, any issue that is or may be in the case.'"
35. <u>Healy v. Spencer</u> , 747 F.3d 1 (1st Cir. 2014).	Pg. 2, ¶ 2	<b><u>The case does not exist as cited.</u></b> Plaintiffs cite to <u>Healey v. Gonzalez</u> , 747 F.3d 111, 121 (1st Cir. 2014). They claim they were referring to <u>Healy v. Spencer</u> , 747 F.3d 1 (1st Cir. 2014).  Plaintiffs quote this case to describe the liberal bounds of discovery, claiming that relevance should be construed "generously," and discovery should not be limited unless the information sought has "no possible bearing" on the claims or defenses.  Neither the quotes nor the propositions they are used to support are found in this opinion, and the proffered quote is contradicted by the relevance and proportionality standard for discovery in Fed. R. Civ. P. 26(b)(1). This opinion is about a Brady claim and the Court does not see any support for Plaintiffs' assertions within.
36. <u>In re Subpoena to Witzel</u> , 531 F.3d 113, 117 (1st Cir. 2008).	Pg. 2, ¶ 3 through pg. 3, ¶ 1	Plaintiffs quote this case to argue that a Fed. R. Civ. P. 26(c) protective order is an extraordinary remedy that requires the moving party to demonstrate "good cause" through a "particular and specific demonstration of fact, as

		<p>distinguished from stereotyped and conclusory statements.”</p> <p>The second quote is not in the opinion and the opinion does not support the propositions raised by Plaintiffs. <u>In re Subpoena to Witzel</u> involved a district court’s denial of a motion to compel and grant of a protective order. The First Circuit affirmed the district court’s denial of the motion to compel, finding that the district court had not abused its discretion in denying the motion. The opinion did not discuss the requirements for a protective order as represented by Plaintiffs.</p>
<p>37. <u>Id.</u></p>	<p>Pg. 6, ¶ 1</p>	<p>Plaintiffs cite this case when stating that Defendants offer no specific evidence, only conclusory assertions, that sixty-eight witnesses would be unmanageable.</p> <p>As stated above, this opinion focused on the denial of a motion to compel and did not discuss protective orders in sufficient depth to support Plaintiffs’ assertions here.</p>
<p>38. <u>DM Rsch., Inc. v. Coll. of Am. Pathologists</u>, 170 F.3d 53, 56 (1st Cir. 1999).</p>	<p>Pg. 4, ¶ 3</p>	<p>Plaintiffs provide a parenthetical for this case citation stating that antitrust claims often require “exploration of the conspirators’ minds and actions.”</p> <p>This quote is not found in the opinion, nor does the opinion support the proposition provided by Plaintiffs. Although this is an antitrust case, the opinion’s discussion of antitrust law at pages 56 and 57 does not make generalized findings that</p>

		antitrust claims require "exploration of the conspirator's minds and actions." Here, the First Circuit affirmed the district court's decision to grant a motion to dismiss on the grounds that the plaintiffs did not plausibly allege specific facts to support an antitrust claim. The court did not go further and discuss the alleged coconspirators' minds and actions.
39. <u>Id.</u>	Pg. 6, ¶ 1	Plaintiff provides a parenthetical for this case stating that antitrust cases often require extensive evidence.  However, the opinion does not support this proposition because <u>DM Rsch, Inc.</u> involved the First Circuit affirming the grant of a motion to dismiss for an antitrust claim where the complaint relied on speculation and generalized language. This dismissal took place before the discovery stage, so discussions of evidence would be premature.
40. <u>Sullivan v. Taglianetti</u> , 588 F.2d 1355, 1357 (1st Cir. 1978).	Pg. 5, ¶ 2	<b><u>The case does not exist as cited.</u></b> The Court could not find the case Plaintiffs were referring to and Plaintiffs acknowledge this may be "misrecalled." (Docket No. 190). The Court cannot evaluate the veracity of this citation.
41. <u>Gill v. Gulfstream Park Racing Ass'n, Inc.</u> , 399 F.3d 391, 401 (1st Cir. 2005).	Pg. 6, ¶ 1	Plaintiffs cite to this case to argue that the First Circuit warns against "arbitrary numerical limits" on witnesses without a showing of oppression or undue burden.  While the opinion does deal with Rule 26, the Court finds no language supporting the specific proposition it is quoted and

		cited in support of. Instead, the opinion discusses an informant's privilege and does not discuss limitations on the number of witnesses a party may call.
42. <u>Whittingham v. Amherst Coll.</u> , 163 F.R.D. 170 (D.Mass. 1995).	Pg. 6, ¶ 2	Plaintiffs characterize this case as one involving a post-discovery ruling, not a preemptive cap on the number of witnesses a party can depose. However, the language of the opinion shows that discovery was ongoing at the time the ruling was issued, not that discovery had already concluded.

<i>Plaintiffs' Response in Opposition to Defendants' Joint Motion for Entry of a Protective and Confidentiality Order and Rule 502(d) Order</i> (Docket No. 176)		
Citation:	Location:	Issue:
43. <u>Pub. Citizen v. Liggett Grp., Inc.</u> , 858 F.2d 775, 789 (1st Cir. 1988).	Pg. 3, ¶ 1	This case is quoted as saying that "[t]he party seeking the protective order must demonstrate that confidentiality is warranted with specific facts, not conclusory statements."  This quote is not found in the opinion nor is the proposition properly supported by the opinion. The opinion discusses the good cause requirement for protective orders barring a party that receives discovery from making it public. Although the existence of a good cause requirement may imply that conclusory allegations are insufficient, there is no language in the opinion to this effect.
44. <u>Id.</u>	Pg. 3, ¶ 2	As in the previous instance, Plaintiffs cite this case as claiming a "particularized showing" is required for a protective order.

		The opinion does not contain this quote. Although the opinion discusses "particular documents" it does not establish the requirement of a "particularized showing."
45. <u>Anderson v. Cyrovac, Inc.</u> , 805 F.2d 1, 7 (1st Cir. 1986).	Pg. 3, ¶ 2	<p>This case is cited for the proposition that discovery should be "as broad as possible," but this quote is not in the opinion.</p> <p>The case contains somewhat similar language providing that "[i]n discovery, the parties are given broad range" on page 12. Plaintiffs state the wrong standard for discovery under Fed. R. Civ. P. 26(b), which imposes relevance and proportionality requirements on discovery. Rule 26(b)(1) states that parties can conduct discovery "regarding any nonprivileged matter that is <b>relevant</b> to any party's claim or defense and <b>proportional</b> to the needs of the case." This standard is not the same as mandating that broad discovery is required.</p>
46. <u>Gill v. Gulfstream Park Racing Ass'n, Inc.</u> , 399 F.3d 391, 401 (1st Cir. 2005).	Pg. 3, ¶ 3	<p><b><u>The case does not exist as cited.</u></b> Plaintiffs cite to <u>Gill v. Gulfstream Aerospace Corp.</u>, 399 F.3d 391, 401 (1st Cir. 2005). They are presumably referring to <u>Gill v. Gulfstream Park Racing Ass'n, Inc.</u>, 399 F.3d 391, 401 (1st Cir. 2005).</p> <p>Plaintiffs cite this case for the proposition that First Circuit policy disfavors "unduly restrict[ing] the flow of discovery," but this quote is not in the opinion. This opinion does discuss how trial courts must balance the burden of proposed discovery against its likely</p>

		benefit, and what constitutes an abuse of discretion in balancing these conflicting interests in discovery.
47. <u>Id.</u>	Pg. 6, ¶ 1	<p>Plaintiffs also use this citation for the principle that including confusing language (here, about the Swiss Penal Code) in a protective order will confuse the discovery process and delay Plaintiffs' access to evidence, contrary to First Circuit efficiency goals.</p> <p>This proposition is not supported by language of the opinion. This case dealt with an interlocutory appeal of a discovery order, and discussed informant's privilege, public interest considerations, confidentiality concerns, and privacy interests. The Court found no language in the opinion supporting Plaintiffs' assertion in its motion. The opinion only discussed "efficiency interests" in the context of when a party can seek an interlocutory appeal.</p>
48. <u>In re Grand Jury Subpoena</u> , 274 F.3d 563, 571 (1st Cir. 2001).	Pg. 4, ¶ 2	Plaintiffs cite this case for the proposition that ethical rules focus on actual conflicts, not hypothetical risks. However, the opinion does not support this argument because this case involved a motion to quash a subpoena and an underlying dispute over attorney-client and work product privileges. It does not align clearly with Plaintiffs' arguments in the instant case.
49. <u>United States v. Gannett Co.</u> , 835 F.2d 392, 395 (1st Cir. 1987).	Pg. 4, ¶ 3	<b><u>The case does not exist as cited.</u></b> Plaintiffs are presumably referring to <u>United States v. Gannett Co., Inc.</u> , No. 13-CV-1984, 2014 WL 6844302 (D.D.C. Nov. 18, 2014) or <u>United States</u>

		<p><u>v. Gannett Co., Inc.</u>, No. 13-CV-1984, 2014 WL 2704109 (D.D.C. Apr. 24, 2014)</p> <p>Plaintiffs' parenthetical for this citation states that disqualification is not required unless the representation is "materially adverse" to the client. The quotation "materially adverse" is not found in either of the aforementioned opinions nor is it supported by them. While these are antitrust cases, neither case discusses disqualification of counsel.</p>
50. <u>Poliquin v. Garden Way, Inc.</u> , 989 F.2d 527, 532 (1st Cir. 1993).	Pg. 4, ¶ 4	<p>Plaintiffs cite this case as stating that a "specific demonstration of need" is required for a protective order.</p> <p>This quote is not in the opinion. However, the case does provide that more than good cause is required to justify protecting discovery material after it is introduced at trial.</p>
51. <u>In re Grand Jury Subpoena</u> , 646 F.3d 159, 164 (4th Cir. 2011).	Pg. 5, ¶ 4	<p><b>Incorrect citation.</b> This case is in the Fourth Circuit, not the First Circuit, as represented by Plaintiffs. This case is properly cited as: <u>In re Grand Jury Subpoena</u>, 646 F.3d 159, 164 (4th Cir. 2011).</p> <p>The proposition this case is cited for is not supported by language in the opinion. Plaintiffs' parenthetical indicates this case is cited in support of the permissive nature of the Hague Evidence Convention. However, this case makes no mention of this convention, only an unnamed Mutual Legal Assistance Treaty.</p>

52. <u>Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa</u> , 482 U.S. 522, 539-40 (1987).	Pg. 5, ¶ 4	This citation is used to support that Hague procedures are "permissive."  This quoted word is not found on pages 539-40, but similar language is found on both pages 535 and 536.
--	------------	---

*Plaintiffs' Supplement to Response in Opposition to Defendants' Joint Motion for Entry of a Protective and Confidentiality Order and Rule 502(d) Order*  
(Docket No. 177)

Citation:	Location:	Issue:
53. <u>United States v. Angiulo</u> , 897 F.2d 1169, 1190 (1st Cir. 1990).	Pg. 2, ¶ 2	Plaintiffs cite this case for the proposition that it condemns "efforts to interfere with witnesses as contrary to fair adjudication."  The proposition this case is somewhat supported by language in the opinion. Pages 1192 and 1193 discuss witness intimidation, albeit in the context of criminal cases and prosecutorial misconduct.
54. <u>Rozier v. Ford Motor Co.</u> , 573 F.2d 1332, 1346 (5th Cir. 1978).	Pg. 3, ¶ 3	This case is cited to assert that broad discovery is essential to prevent "trial by ambush," but this quote is not in the opinion.  Similar language explaining that liberal discovery rules aim to make trial "less of a blind man's bluff and more a fair contest[.]" is found on this page. However, Plaintiffs misstate the state of the law regarding discovery. Fed. R. Civ. P. 26(b)(1) states that parties can conduct discovery "regarding any nonprivileged matter that is <b>relevant</b> to any party's claim or defense and <b>proportional</b> to the needs of the

		<p>case." This is not the same as mandating that broad discovery is essential.</p>
<p>55. <u>Anderson v. Cyrovac, Inc.</u>, 805 F.2d 1, 7 (1st Cir. 1986).</p>	<p>Pg. 4, ¶ 1</p>	<p>This case is cited for the proposition that discovery should be "as broad as possible," but this quote is not in the opinion.</p> <p>Rather, on page 12, this case provides that "[i]n discovery, the parties are given broad range." As stated above, Plaintiffs misstate the state of the law regarding discovery by stating that discovery should be "as broad as possible." Fed. R. Civ. P. 26(b)(1) states that parties can conduct discovery "regarding any nonprivileged matter that is <b>relevant</b> to any party's claim or defense and <b>proportional</b> to the needs of the case." It contradicts Fed. R. Civ. P. 26 to say that discovery is as broad as the parties can make it.</p>

---

End of Document



Portfolio Media, Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com  
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# 5 Things To Know As California Courts Decide On AI Rule

By **Emily Sawicki**

Law360 (July 17, 2025, 4:47 PM EDT) -- Fourteen months after California Supreme Court Chief Justice Patricia Guerrero first convened a task force to study potential benefits and risks of using artificial intelligence in the court system, the Judicial Council of California is poised Friday to consider the proposed rules and standards the task force developed.

If approved, the new parameters will govern how the country's largest state court system will navigate the use of generative AI for court-related tasks, in a move to "help promote responsible innovation in court operations while protecting confidential information, ensuring appropriate oversight, and maintaining public trust in the judicial branch," according to information from council staff.

The new rule would apply to court staff, including state court employees, contractors and volunteers, as well as judicial officers, while the standard dictates its use for judicial officers specifically.

Task force members include its chair, Administrative Presiding Justice Brad Hill of the Court of Appeal, Fifth Appellate District, alongside Justice Carin Fujisaki of the First Appellate District, Judge Kyle Brodie of San Bernardino County Superior Court, Administrative Presiding Justice Mary Greenwood of the Sixth Appellate District, Judge Arturo Castro of Alameda County Superior Court, and council members David Yamasaki and Gretchen Nelson.

If the new rules are approved, they are scheduled to go into effect on Sept. 1.

Here are five things to know before the decision is made.

## **The proposal leaves policy-writing up to individual courts.**

Though the **task force** unveiled a model AI policy in February, its proposal going before the judicial council includes additions to the California Rules of Court and the California Standards of Judicial Administration — leaving it up to individual courts to write their own policies, if they choose to permit AI use at all.

If the judicial council approves the move, courts must adapt the new rule and standard into a policy, or forbid the use of artificial intelligence altogether.

The model policy includes several optional elements that courts may choose to include beyond the scope of the rule and standard. Among them is a requirement for supervisor approval prior to the use of AI, a strong password requirement and a directive to "opt out" of data collection.

Under the proposal, if a court chooses not to forbid the use of AI and not to adopt the model rules, it will have through Dec. 15, 2025, to draft and enact policies in line with the rules and standards.

## **The proposed parameters touch on privacy, avoiding bias, ensuring accuracy and disclosure.**

The new rule, which will be entered as Rule 10.430 if it is adopted, forbids the entry of confidential and nonpublic information into publicly available generative AI systems.

Court staff and judicial officers must also verify the accuracy of any AI-generated material, while taking steps to remove any harmful, biased or offensive content, the proposed rule states. The rule also prohibits the use of AI in discrimination.

The proposed rule requires disclosure of "the use of or reliance on generative AI if the final version of a written, visual or audio work provided to the public consists entirely of generative AI outputs."

The task force initially proposed language stating it is mandatory to disclose the use of AI in most cases if the program's outputs make up a "substantial portion of the content used in the final version of a written or visual work provided to the public."

The task force created a draft proposal, which it circulated for comments in March and April. The initial proposal drew 19 comments across a range of sources including trial courts, law professors, judicial officers, attorney or bar associations, and others.

In light of the ambiguity of the term "substantial portion," the disclosure language was revised after the public comment period closed.

Disclosing use when AI is assisting in tasks, but not used to create a final product, may unnecessarily raise questions of reliability, the task force decided.

### **The standard will allow judges to use AI "for adjudicative tasks."**

Some judges have already begun turning to ChatGPT and other generative AI programs to help craft opinions, notably U.S. Circuit Judge Kevin C. Newsom, **who disclosed** his use of AI in a concurrence he wrote to an Eleventh Circuit ruling in May 2024.

Judge Newsom acknowledged at the time that his use of large language models including ChatGPT, Gemini and Claude might be considered "heresy," but he urged other judicial officers to consider how such programs might aid in their "interpretive analysis" of a case.

The proposal follows this line of thinking, reminding judges "to comply with applicable laws, court policies and the California Code of Judicial Ethics when using generative AI," but otherwise permitting its use if rules and standards are followed.

About 1 in 3 public comments collected urged the task force to prohibit judges' use of artificial intelligence in drafting opinions and orders, and one suggested generative AI should be used only for "nonjudicial, public facing applications" like document retrieval, according to the staff report.

Both judges who weighed in told the task force not to adopt the rule and standard, though for different reasons: one said existing rules and laws already cover the issue, while the other said that aside from forbidding its use for adjudicative purposes, it was too early to create other parameters.

The task force determined it was better to hand control over to judicial officers, saying that courts and judges "are in the best position to identify acceptable uses of generative AI to meet their specific needs." But even seemingly straightforward guidance, like a ban on using AI to create the substance of an adjudicative decision, may be unintentionally broad when judges may use a program for research or analysis, or even to check grammar, the task force pointed out.

"While it is likely uncontroversial to say that judicial officers should not prompt ChatGPT to decide issues or draft an opinion for them, it is less clear whether and to what extent it is acceptable for judicial officers to use generative AI tools for tasks like researching and outlining legal arguments," the task force stated in the staff report.

"The task force therefore concluded that judicial officers should have the discretion to decide whether specific uses of generative AI are appropriate for adjudicative tasks," the task force added, so long as they align with ethics rules.

The proposed standard urges judges to "take reasonable steps" to verify information and remove offensive or biased information. The standard also directs judicial officers not to use AI to discriminate and not to enter protected information into a public system.

## **The task force kicked judicial ethics questions to the state Supreme Court.**

The "task force recognizes that the possibility that generative AI might be used to draft orders, opinions, and other adjudicative materials raises significant concerns," according to the staff report. "However, the task force concluded that this issue is more appropriately addressed by the California Code of Judicial Ethics and related ethical guidance."

Several times in the staff report, the task force expressed its expectation that rules and guidance will continue to develop alongside generative artificial intelligence itself, including ethics standards.

"For example, the canons prohibit judicial officers from abrogating their responsibility to personally decide the matters before them and considering evidence and facts that were not properly judicially noticed, and require judicial officers to 'act at all times in a manner that promotes public confidence in the integrity and impartiality of the judiciary,'" the task force stated, adding that the "canons therefore likely prohibit judicial officers from having generative AI decide issues or write their opinions for them, and that the Supreme Court's judicial ethics committees are the appropriate bodies to ask for guidance on this subject."

## **California's proposed rules follow industry standards.**

As proposed, the new ethics rules fall in line with norms that have arisen since the advent of generative artificial intelligence, aligning closely with a policy adopted in **December 2024** by the Illinois Supreme Court for the state's courts and an interim policy Delaware courts announced **last October**.

The Illinois rules acknowledge that AI use "may be expected" by court staff, attorneys, litigants and judges, and proposes guidelines to ensure accuracy and protect sensitive information.

Similarly, the brief Delaware policy authorizes court staff and judicial officers to use AI, but emphasizes their individual responsibility for the accuracy of the program's output.

However, the interim Delaware policy goes further than the California proposal, specifically mandating that authorized users "may not delegate their decision-making function to approved Gen AI," and requiring training.

In California, the task force said it was considering a training mandate, but none is included in the current proposal.

--Additional reporting by Hope Patti, Lauraann Wood and Lauren Berg. Editing by Robert Rudinger.

## Attorney sanctioned \$10 for AI hallucinated case citations

By [Grace Barbic](mailto:gbarbic@lawbulletinmedia.com) gbarbic@lawbulletinmedia.com

Posted July 18, 2025 11:44 AM CDT

In one of the first known instances of its kind in Illinois state court, a defense attorney who used ChatGPT for assistance with writing a motion must pay a \$10 sanction because the filing included 12 hallucinated case citations.

As generative artificial intelligence rapidly develops and becomes more widely used in the legal community, dozens of courts across the country are facing similar issues with fake citations.

The [Illinois Supreme Court](#) embraces the use of AI in legal practice and authorizes its use by litigants, attorneys, judges, judicial clerks, research attorneys and court staff, but only if the use is compliant with legal and ethical standards.

The high court issued a policy in December requiring all users to “thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations” and that “users must understand both general AI capabilities and the specific tools” before using any AI technology.

In an eight-page order penned by Cook County Circuit Court Judge [William B. Sullivan](#) of the [Chancery Division](#) Wednesday, a defendant’s motion to dismiss was stricken without prejudice because the attorney submitted nonexistent case citations.

The attorney, [Danielle N. Malaty](#), was found to have violated Illinois Supreme Court Rule 137, and Sullivan imposed a sanction of \$10.

Malaty was working for [Goldberg Segalla](#) at the time, but her information is no longer available on the firm’s website. The firm’s media contact could not be reached.

Sullivan found that Malaty failed to make a reasonable inquiry into whether the citations she used actually existed, noting that the submission was “particularly egregious.”

Noemi Calderon sued Dynamic Manufacturing Inc. for employment discrimination in [Cook County Circuit Court](#).

Leading up to a hearing on Dynamic’s motion to dismiss, the court learned through communication with Dynamic’s then-counsel Malaty that the motion and reply she filed contained cases made up or misapplied by ChatGPT, a generative AI tool.

Among the 12 hallucinated cases, some did not exist at all, while a few were real cases unrelated to the proposition they were cited for or they cited the wrong court, confusing federal and state authority.

The court conducted an evidentiary hearing on the imposition of sanctions pursuant to Rule 137, which mandates that an attorney must sign court documents to certify that they read the document.

The rule also mandates that the signature certifies that “to the best of the attorney’s knowledge, information and belief formed after reasonable inquiry ... the document is well grounded in fact and is warranted by existing law or a good-faith argument for the extension, modification or reversal of existing law.”

At the hearing, Malaty said she has been using AI in her legal practice since January.

She said she knew it was “limited” and could not replace a human lawyer but found using it “akin to brainstorming with a fellow lawyer,” documents stated.

Malaty explained that she would prompt AI to generate a “first draft,” which she reviewed and edited for factual accuracy, overall analysis and style.

However, in this instance, she submitted the motion without checking the accuracy of the case captions.

She admitted that she only checked case citations when something in the analysis stood out to her as unfamiliar or wrongly stated, documents said.

Malaty explained she was the only attorney working on the case and had been “particularly busy” and “under a time crunch.” She expressed remorse to the court and to the plaintiff’s counsel, documents stated.

In mitigation, Malaty said she took 7.25 hours of continuing legal education on AI. She also said she paid plaintiff’s counsel \$1,000 in compensation for time spent on the hallucinated citations with plans for additional reimbursement.

Sullivan took all of this into consideration when making his decision — balancing the severity of the violation, Malaty’s demonstrated intent to right her wrongs and the interest in deterrence, he noted.

“Ruling on Dynamic’s Motion would launder nonexistent case law and legitimize hallucinated authorities,” Sullivan wrote. “That would be intolerable to a judicial system founded on the common-law principles of precedent and *stare decisis*.”

Sullivan said the court “deeply appreciates” the steps Malaty has already taken to compensate the plaintiff and educate herself about AI.

“However, completely absolving Malaty based on her post-violation actions does not deter irresponsible AI use in the first instance,” Sullivan wrote.

Malaty claimed she did not know AI could “hallucinate” legal authority, but she had heard about it in news headlines and was aware that it could generate “incorrect statements.”

“Knowing that AI could provide any inaccurate content, a reasonable attorney would have ensured that all AI-generated content was grounded in existing law before filing such content with a court,” Sullivan wrote. “A reasonable attorney would have been cognizant of her duties of technological competence and candor to the tribunal when using technology with which she had little experience.”

Sullivan also noted that an attorney cannot reasonably rely on AI-generated citations alone. He found that doing so would be the equivalent of accepting conclusory statements without doing any investigation, he wrote.

Sullivan cited *Mata v. Avianca Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023) in highlighting the harms that can be caused by the use of hallucinated citations.

Those harms include wasted time and money, potential harm to the reputation of judges and courts whose names are falsely invoked as authors of bogus opinions, the promotion of cynicism about the legal profession and the fact that a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity.

Malaty could not be reached for comment.

The case is *Calderon v. Dynamic Manufacturing Inc.*, No. 2024 CH 09839.

Practice Areas: [Professional Liability](#)

© 2025 by Law Bulletin Media. Content on this site is protected by the copyright laws of the United States. The copyright laws prohibit any copying, redistributing, or retransmitting of any copyright-protected material. The content is NOT WARRANTED as to quality, accuracy or completeness, but is believed to be accurate at the time of compilation. Websites for other organizations are referenced on this site; however, Law Bulletin Media does not endorse or imply endorsement as to the content of these websites. By using this site you agree to the [Terms, Conditions and Disclaimer](#). Law Bulletin Media values its customers and has a [Privacy Policy](#) for users of this website.



---

Portfolio Media, Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com  
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

---

## Atty Apologizes For Citation Error In IP Dispute

By **Andrea Keckley**

Law360 (August 12, 2025, 4:26 PM EDT) -- A New York attorney who became one of many accused of using generative artificial intelligence for a brief after a federal judge found citations to nonexistent cases apologized Tuesday for a mistake in a more recent brief flagged for a false citation.

Solo practitioner Steven A. Feldman, the lawyer for Affable Avenue LLC in an ongoing intellectual property lawsuit filed by Flycatcher Corp. Ltd., told U.S. District Judge Katherine Polk Failla, "I deeply regret this clerical error."

An attorney for co-defendant Top Experience Co., Joel G. MacMull of Mandelbaum Barrett PC, told the court on Monday, "Unfortunately, we must write the court once more in connection with attorney Steven Feldman's filings with the court based on our continued ethical obligations" under the New York Rules of Professional Conduct.

That filing flagged an erroneous citation to a D.C. federal court case, *Himmelstein v. Comcast of the District LLC*, in Feldman's Aug. 8 memo in support of the lawsuit's dismissal. In a letter to the court on Tuesday, Feldman said he meant to cite *Himmelstein v. Matthew Bender & Co.*, a New York state court case.

Matthew Bender is a LexisNexis company; Law360 is owned by LexisNexis Legal & Professional, a RELX company.

The erroneous citation, Feldman said, "was regrettably introduced during a final verification of the citation string while double-checking and preparing the citations and table of authorities."

"That said, Mr. MacMull's letter brings to the fore a significant challenge I have been struggling with throughout this litigation concerning the verification of unreported citations, familiar to the courts and the bar — the pervasive use of proprietary, nonneutral reporters such as Westlaw and [LexisNexis] when an official, publicly accessible version is unavailable or when the proprietary source is simply wrong," he added.

Feldman did not immediately respond to Law360's request for comment.

The letter came as the parties prepared to appear in court again later this month. Back in June, Judge Failla ordered Feldman to explain why his brief in support of Affable's motion to toss the lawsuit shouldn't be dismissed after she suspected him of using AI to write it due to its citations of nonexistent cases.

Feldman's response again drew the suspicion of Judge Failla, who **said** that it contained a quote from a case in which that quote didn't appear. Rather, it was from an article about the case.

"Mr. Feldman did not attribute the quote to this article," she wrote. "That is especially concerning considering that he was responding to an order to show cause why he should not be sanctioned for his erroneous citations."

Feldman's July 11 response acknowledged that his brief's errors "resulted from sophisticated AI hallucination mechanisms rather than intentional misconduct." After writing of ancient scribes who "carried their stylus as both tool and sacred trust," he went on to say, "I pray that through comprehensive correction and unwavering diligence going forward, I may prove myself worthy to carry the stylus once more in service of justice and truth."

Affable's motion to dismiss the lawsuit remains pending. The court initially scheduled parties in a July order to appear in court on Aug. 14, but the hearing was rescheduled for Aug. 22.

"The court wants to hear directly from Mr. Feldman," Judge Failla wrote in July, "so that it can give him the opportunity to — as he puts it — 'prove [himself] worthy to carry the stylus once more in service of justice and truth.'"

Plaintiff Flycatcher Corp. Ltd. is represented by Tal S. Benschar and Efrem T. Schwalb of Koffsky Schwalb LLC.

Defendant Affable Avenue LLC is represented by Steven A. Feldman of the Law Office of Steven A. Feldman & Associates PLLC.

Top Experience Company LLC is represented by Joel Geoffrey MacMull and Brian Block of Mandelbaum Barrett PC.

The case is Flycatcher Corp. Ltd. et al. v. Affable Avenue LLC et al., case number 1:24-cv-09429, in the U.S. District Court for the Southern District of New York.

--Additional reporting by Jack Karp. Editing by Robert Rudinger.

---

All Content © 2003-2025, Portfolio Media, Inc.

[FINDLAW](#) / [CASE LAW](#) / [GEORGIA](#) / [GA CT. APP.](#) / SHAHID V. ESAAM

## SHAHID v. ESAAM

### Court of Appeals of Georgia.

SHAHID v. ESAAM.

**A25A0196**

**Decided: June 30, 2025**

**Vic Brown Hill, Marietta, for Appellant. Diana Lynch, Atlanta, for Appellee.**

After the trial court entered a final judgment and decree of divorce, Nimat Shahid (“Wife”) filed a petition to reopen the case and set aside the final judgment, arguing that service by publication was improper. The trial court denied the motion, using an order that relied upon non-existent case law. For the reasons discussed below, we vacate the order and remand for the trial court to hold a new hearing on Wife’s petition. We also levy a frivolous motion penalty against Diana Lynch, the attorney for Appellee Sufyan Esaam (“Husband”).

According to Wife’s October 2023 verified petition to reopen case, Husband filed a complaint for divorce in April 2022, service was performed by publication, and the trial court entered a final judgment in July 2022. In the petition, Wife averred that she had moved to Texas after she and Husband separated in July 2021 and that Husband failed to use reasonable diligence to determine her whereabouts before obtaining service by publication of his divorce complaint. Following a hearing, the superior court denied Wife’s motion. We granted Wife’s application for discretionary review, and this appeal followed.

1. Citing *Reynolds v. Reynolds*,<sup>1</sup> Wife argues that the superior court erred when it denied her petition to reopen the case and set aside the divorce decree because Husband did not make a sufficient showing of due diligence to allow service by publication under OCGA § 9-11-4 (f). Wife points out in her brief that the trial court relied on two fictitious cases in its order denying her petition, and she argues that the order is therefore, “void on its face.”

In his Appellee's Brief, Husband does not respond to Wife's assertion that the trial court's order relied on bogus case law. Husband's attorney, Diana Lynch, relies on four cases in this division, two of which appear to be fictitious, possibly "hallucinations" made up by generative-artificial intelligence ("AI"),<sup>2</sup> and the other two have nothing to do with the proposition stated in the Brief.<sup>3</sup>

Undeterred by Wife's argument that the order (which appears to have been prepared by Husband's attorney, Diana Lynch) is "void on its face" because it relies on two non-existent cases, Husband cites to 11 additional cites in response that are either hallucinated or have nothing to do with the propositions for which they are cited. Appellee's Brief further adds insult to injury by requesting "Attorney's Fees on Appeal" and supports this "request"<sup>4</sup> with one of the new hallucinated cases.

We are troubled by the citation of bogus cases in the trial court's order. As the reviewing court, we make no findings of fact as to how this impropriety occurred, observing only that the order purports to have been prepared by Husband's attorney, Diana Lynch. We further note that Lynch had cited the two fictitious cases that made it into the trial court's order in Husband's response to the petition to reopen, and she cited additional fake cases both in that Response and in the Appellee's Brief filed in this Court.

As noted above, the irregularities in these filings suggest that they were drafted using generative AI. In his 2023 Year-End Report on the Federal Judiciary, Chief Justice John Roberts warned that "any use of AI requires caution and humility."<sup>5</sup> Roberts specifically noted that commonly used AI applications can be prone to "hallucinations," which caused lawyers using those programs to submit briefs with cites to non-existent cases.<sup>6</sup>

Although the present case may be the first occasion for a Georgia appellate court to confront the problems that can flow from a lawyer's apparent adoption of generative-AI, other courts have commented on the issue. In a 2023 opinion, a federal district court noted in *Mata v. Avianca, Inc.*, that "there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings."<sup>7</sup> In that case, the attorneys had abandoned their responsibilities when they submitted non-existent judicial opinions with fake quotes and citations created by the AI tool ChatGPT, then continued to stand by the fake opinions after judicial orders called their existence into question.<sup>8</sup>

Indeed,

[m]any harms flow from the submission of fake opinions. The opposing party wastes time and money in exposing the deception. The Court's time is taken from other important endeavors. The client may be deprived of arguments based on authentic judicial precedents. There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the

reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity.<sup>9</sup>

Here, as in *Mata*, Lynch's use of fictitious cases and citations has deprived the opposing party of the opportunity to appropriately respond to her arguments.

As to Lynch's request for attorney fees "for the costs incurred in responding to this appeal[,]" that section of Appellee's Brief provides:

1. OCGA § 9-15-14: This statute authorizes the recovery of attorney's fees if the court finds that an action, including an appeal, lacked substantial justification or was filed to delay or harass.
2. *Johnson v. Johnson*, 285 Ga. 408 (2009): The court awarded attorney's fees to the prevailing party in a divorce appeal, finding that the appeal was without merit and amounted to frivolous litigation.

We cannot find the cited case, *Johnson v. Johnson*, either by case name or citation. And, not surprisingly, we could not locate the case by its purported holding, which is a blatant misstatement of the law. More than 30 years ago, this Court held that "OCGA § 9-15-14 does not authorize the imposition of attorney fees and expenses of litigation for proceedings before an appellate court of this state."<sup>10</sup> Since then, our Supreme Court has consistently and clearly reiterated this point multiple times: "attorney's fees incurred in connection with appellate proceedings are not recoverable under OCGA § 9-15-14."<sup>11</sup>

Moreover, it is worth pointing out that we granted Wife's application for discretionary review (Case Number A25D0396) which "established as a matter of fact and law that her appeal is not frivolous."<sup>12</sup> "As used in [OCGA § 9-15-14], 'lacked substantial justification' means substantially frivolous, substantially groundless, or substantially vexatious." OCGA § 9-15-14 (b). Thus, even if OCGA § 9-15-14 were an appropriate avenue to recover attorney fees for the costs of defending a frivolous appeal, our grant of Wife's application should have prompted Husband to reconsider his approach before filing the Appellee's Brief.

Under the circumstances and given the indisputably clear state of the law, Husband's attorney, Diana Lynch, cannot reasonably have believed, as the Appellee's Brief "requests," that this Court would "award attorney fees under OCGA § 9-15-14 for the costs incurred in responding to this appeal." Further, Lynch provided no other basis for an award of "attorney's fees to the prevailing party in a divorce appeal," other than a fictitious case, which purported to be a 2009 case from the Supreme Court of Georgia.

To be clear, we make no factual finding as to who (or what) inserted the fictitious cases into the superior court's order.<sup>13</sup> We are deeply troubled, however, that Lynch submitted to this Court an Appellee's Brief,

completely ignoring the second of two arguments that Wife raised in her Appellant's Brief and Application for Discretionary Review (wherein Wife pointed out the two fictitious cases in the trial court's order),<sup>14</sup> and provided 11 bogus case citations <sup>15</sup> out of 15 total,<sup>16</sup> one of which was in support of a frivolous request for attorney fees.

Therefore, we impose a \$2,500 frivolous motion penalty on Lynch, which is the most the law allows, pursuant to Court of Appeals Rule 7 (e) (2).<sup>17</sup> We have no information regarding why Appellee's Brief repeatedly cites to nonexistent cases and can only speculate that the Brief may have been prepared by AI.

2. As to Wife's argument that the trial court erred by denying her petition to reopen case, we are unable to conduct meaningful review of that ruling.

In the Appellee's Brief, Husband argues that the superior court's factual findings are not reviewable because Wife failed to cause a transcript of the court's hearing to be included with the Record on Appeal.

It is true that "where an appeal is taken which draws in question the transcript of the evidence and proceedings, it shall be the duty of the appellant to have the transcript prepared at the appellant's expense."<sup>18</sup> Thus, the general rule is that "in the absence of a transcript or legal substitute for a transcript, "there is no evidence before [the appellate] court and the judgment of the trial court on evidentiary matters cannot be reviewed." However, this rule is based on the presumption that trial courts follow the law, and that presumption can be rebutted.<sup>19</sup> "[T]he absence of a transcript does not authorize such presumption of correctness when the record plainly shows harmful error."<sup>20</sup>

In this case, Wife has rebutted the presumption of regularity by pointing out that both of the cases cited in the order denying her petition to reopen do not exist.<sup>21</sup> Because the order denying her motion to set aside the divorce decree has a defect apparent on its face, we cannot conduct any meaningful appellate review of the merits of Wife's argument that the court lacked jurisdiction over her person.<sup>22</sup> Accordingly, we vacate the order and remand for further proceedings consistent with this opinion. The superior court is specifically directed to hold a new hearing on Wife's motion to set aside the divorce decree.

3. In sum, we vacate the superior court's order and remand for further proceedings, including a new hearing on Wife's motion to reopen. We also impose a \$2,500 penalty against Lynch. This penalty shall constitute a money judgment in favor of Wife (Nimat Shahid) against Husband's attorney (Diana Lynch), and the trial court is directed to enter judgment in such amount upon return of the remittitur in this case.<sup>23</sup>

Judgment vacated and case remanded.

# Atty Had 6 AI Tools Check Each Other, Yet Fakes Still Cited

By **Andrea Keckley**

Law360 (November 21, 2025, 4:03 PM EST) -- A California federal judge has sanctioned a solo practitioner representing the plaintiffs in a proposed wage and hour class action against clothing brand Vuori Inc. after he admitted to using about a half-dozen artificial intelligence tools to prepare a motion.



U.S. Magistrate Judge Nathanael M. Cousins found James Dal Bon to be inadequate class counsel for his use of AI, referred him to the court's professional conduct committee, struck the at-issue motions and fined him \$250 on Thursday. He then scheduled the case to go to trial in July. (Klaus Ohlenschlaeger via Alamy)

Despite James Dal Bon using the different tools to check each other's work, his filing late last month for preliminary approval of a settlement included a memorandum containing eight hallucinated quotes and one non-existent case, according to court documents.

U.S. Magistrate Judge Nathanael M. Cousins found Dal Bon to be inadequate class counsel, referred him to the court's professional conduct committee, struck the at-issue motions, and fined him \$250 on Thursday. He then scheduled the case to go to trial in July.

Dal Bon is just the latest of many attorneys to face potential professional consequences for their use of artificial intelligence in the process of drafting court filings. Less than a week ago, another solo practitioner **was hit with a \$500 fine** for submitting a hallucination-filled brief in a wage suit.

Such blunders, however, haven't always led to sanctions. Earlier this month, for instance, an Oregon federal judge **declined to sanction** Buchalter PC and other counsel representing an environmental nonprofit in a trademark dispute for their use of AI in a filing.

Dal Bon runs San Jose, California-based Wisdom Law Group APC and says he often provides sole representation to plaintiffs in lawsuits against major companies with scores of attorneys. He has admitted to and expressed remorse for his use of AI, saying in a response Nov. 12 to the court's show-cause order that this "was [his] first attempt to incorporate artificial intelligence tools extensively in drafting a complex class action motion."

Dal Bon offered to forfeit all attorney fees to the class, asking the court to consider that as an alternative to imposing sanctions. Judge Cousins declined the request.

"While the court appreciates Dal Bon's 'transparency and candor in admitting the unverified use of AI as the explanation for the false citation,' these errors are highly problematic and simply unacceptable to the court, especially given that there have been many recent and highly publicized cases where attorneys' use of artificial intelligence has resulted in briefs that cite non-existent or hallucinated authorities," Judge Cousins said Thursday. "This is especially so given that Dal Bon 'acknowledge[s] that the tools come with warning labels concerning hallucinations.' False case citations have real harms, including creating unnecessary work for courts and opposing parties, undercutting client advocacy, and diminishing trust in the judicial system."

The lawsuit — filed by one of Vuori's former hourly employees, Terrence Buchanan — accuses Vuori of miscalculating the overtime paid to its employees by failing to account for commissions or bonuses in its calculations. The proposed settlement would have seen Vuori pay \$1.1 million to about 2,895 current and former retail employees.

Dal Bon did not immediately respond to Law360's request for comment Friday.

Buchanan is represented by James Dal Bon of Wisdom Law Group APC.

Vuori is represented by Lindsay Hutner and Samuel S. Hyde of Greenberg Traurig LLP.

The case is Buchanan v. Vuori Inc., case number 5:23-cv-01121, in the U.S. District Court for the Northern District of California.

--Additional reporting by Emily Sawicki and Rose Krebs. Editing by Janice Carter Brown.

# Calif. Bill Would Ban AI From Replacing Arbitrators' Analysis

By **Emily Sawicki**

Law360 (January 14, 2026, 3:11 PM EST) -- A bill introduced in the California state Senate seeks to regulate attorneys' use of generative artificial intelligence statewide, including banning lawyers from entering private client information into public AI systems and prohibiting arbitrators from utilizing AI in decision-making.

The legislation, known as Senate Bill 574, would also require lawyers take "reasonable steps" to ensure the accuracy of AI-generated content.

The bill was authored by state Sen. Tom Umberg, a Democrat representing Orange County, who said in a statement that the bill is part of a package "about accountability, fairness, and making sure Californians are protected as our systems and technologies change." A former prosecutor, Umberg is now a trial attorney and name partner at Umberg Zipser LLP, and also chairs the California Senate Judiciary Committee.

Umberg announced the bill package on Jan. 8, after submitting it on Jan. 5.

"Artificial Intelligence and its use now permeate every industry in the U.S.," Umberg said in written comments presented to the Senate Judiciary Committee. "Its capabilities continue to improve at an exponential rate, but it is far from perfect."

"We must be cautious when determining best practices for its use in high-stakes industries, including the legal profession," Umberg said. "SB 574 protects those receiving legal services by codifying certain safeguards for the use of A.I. by attorneys and arbitrators."

Speaking with Law360 Wednesday, Umberg said he drafted the legislation based on recent experiences he has had practicing. Not only has he personally come across filings with nonexistent cases cited and other errors, Umberg said, but he has had law partners, judges and arbitrators raise their concerns to him about irresponsible use of the technology.

"The use of artificial intelligence is becoming more prevalent in everything in life, particularly in law, because it is so much founded on collections of data and other information from a database, that it makes it very attractive to use artificial intelligence to engage in shortcuts," Umberg said. "While it may certainly be useful for research, it still requires that a human being actually make sure that whatever they're submitting to the court and whatever the court submits to the litigants is accurate."

The bill notes that existing law requires court filings to be signed by the attorney of record if a party is represented. It prohibits such briefs, pleadings, motions and other filings from "containing any citations that the attorney responsible for submitting the pleading has not personally read and verified, including any citation provided by generative artificial intelligence."

Likewise, the proposed bill bans neutral arbitrators from relying on AI to aid in their decision-making process. If an arbitrator does use information provided by AI, they must notify parties ahead of time of their use of the system, under the legislation, which also states arbitrators must be responsible for all aspects of awards, whether they used AI or not.

"The use of generative artificial intelligence tools by arbitrators shall not replace their independent analysis of the facts, the law, and the evidence," the proposed bill text states in part. "An arbitrator

shall not relinquish their decision-making powers to generative artificial intelligence and shall avoid delegating any tasks to generative artificial intelligence tools if such use could influence procedural or substantive decisions."

Umberg said Wednesday that the essence of the bill boils down to maintaining the integrity of the judicial process.

"The aim of the bill is to make sure that as artificial intelligence becomes more prevalent and more useful, that the process has human accountability and the integrity of the process that currently exists is maintained," Umberg said.

Analysis by the California Senate Judiciary Committee found that the bill was unlikely to be preempted by the Federal Arbitration Act, as it does not affect the arbitration itself, but provides guidelines for the use of AI.

As of Jan. 10, when the initial bill analysis was entered into the public record, SB 574 had no known opponents. The legislation is now before the judiciary, appropriations and rules committees. Umberg noted the bill's progress is just beginning, anticipating future drafts are likely to be refined as his colleagues weigh in.

--Editing by Alex Hubbard.

# Calif. Justices Order Prosecutors To Explain Alleged AI Errors

By **Dorothy Atkins**

Law360 (January 15, 2026, 4:28 PM EST) -- The California Supreme Court has ordered Nevada County prosecutors to explain to a lower court why they shouldn't be sanctioned for "apparent serial submission" of artificial intelligence-generated briefs with nonexistent legal citations in multiple criminal proceedings.

In a Wednesday docket order, the justices granted Kyle Kjoller's Oct. 30 petition for review. The petition asked the justices to consider whether prosecutors working under Nevada County District Attorney Jesse Wilson should be ordered to explain why they shouldn't face sanctions for filing error-filled briefs in multiple criminal proceedings that were allegedly created using artificial intelligence tools.

Nevada County is northeast of Sacramento and north of Lake Tahoe in the Sierra Nevada. It includes Nevada City, known for its historic gold rush-era downtown, and the popular ski town of Truckee.

In granting the petition, the justices also sent the case back to the Third Appellate District of the Court of Appeal, with directions for it to vacate its Oct. 20 order summarily denying Kjoller's motion for sanctions against the prosecutors. The justices said the intermediate appellate court must issue a new order directing the Nevada County district attorney to explain why sanctions should not be imposed.

"The Court of Appeal may appoint a referee to hear evidence and make findings on certain specified questions," the justices added.

Kjoller's counsel and representatives for the Nevada County District Attorney's Office did not immediately respond to requests for comment on Thursday.

The trip to the Golden State's top court is the latest development in a fast-moving legal proceeding over Kjoller's emergency request for a writ of habeas corpus after he was incarcerated without bail last spring as he faced multiple counts of illegal gun possession.

Kjoller's petition, which has drawn **amicus support** from nearly two dozen law professors and the California Public Defenders Association, argued that the Nevada County District Attorney's Office has filed briefs citing fabricated authority in at least three criminal cases in recent months, including in Kjoller's case, but county prosecutors have repeatedly denied that they used AI to create the briefs.

Kjoller claims prosecutors have instead offered "questionable, inconsistent and incoherent justifications" for the errors, while minimizing their alleged misconduct and repeatedly accusing a public defender of misconduct for asking the court to investigate the errors.

Lower courts twice denied Kjoller's requests for an order to show cause why the prosecutors should not face sanctions, and Kjoller alleges that even after the lower courts' denials, prosecutors filed two more briefs with fabricated citations and quotes in other criminal cases.

The prosecutors' error-filled document at issue in Kjoller's case was filed Sept. 4 in response to Kjoller's petition challenging his pretrial incarceration, which the intermediate appellate court ultimately agreed was unlawful, according to court documents.

In the Sept. 4 filing, the district attorney's office asked the court to deny Kjoller's emergency petition for writ of habeas corpus. However, the filing, which was signed under penalty of perjury by Deputy District Attorney Madison Maxwell, allegedly cited at least three fake cases that do not exist and three other cases that do exist, but do not stand for the principle the district attorney claimed, Kjoller said in his petition. The prosecutor's filing also repeatedly cited a real constitutional provision on restitution, but inaccurately claimed it supported the prosecutor's incarceration arguments, Kjoller said.

On Sept. 17, Kjoller's counsel filed a sanctions motion, expressing concerns that the errors were AI-generated and asking the court to strike the filing, sanction prosecutors and award defense counsel fees for their time spent on the motion, Kjoller's petition said. But Maxwell's supervisor, Assistant District Attorney Lydia Stuart, allegedly called Kjoller's counsel directly to try to convince him to withdraw the sanctions motion and suggested that he would be subject to ethics violations for pursuing the motion, purportedly without good cause, according to Kjoller's petition.

Kjoller called on the courts to order an investigation into the prosecutors' conduct, arguing that it poses serious threats to the integrity and legitimacy of the criminal system, particularly since both Stuart and Maxwell have each filed additional briefs in other criminal cases with errors that appear to be created by AI.

In a Nov. 21 amici curiae letter, prominent legal scholars backed Kjoller in asking the state justices to take up the case. The letter noted that although there are already hundreds of published cases that have grappled with errors from AI-generated briefs and the "cascading risks to the rule of law," this case is the first known allegation of a prosecutor's office repeatedly filing briefs with nonexistent and misleading legal authority that appear to be generated by AI.

If the allegations are true, such misconduct violates not only the California Rules of Court, but also the district attorney's ethical obligations, and it poses grave risks to the constitutional rights of criminal defendants, according to the letter.

The scholars who signed the letter include San Francisco's ousted district attorney, Chesa Boudin, who is currently executive director of the Criminal Law and Justice Center at the University of California, Berkeley School of Law; and Barry Scheck, professor at Yeshiva University's Benjamin N. Cardozo School of Law, who co-founded The Innocence Project, a group that works to exonerate those who have been wrongfully convicted.

Scheck told Law360 on Thursday that he's thrilled with the state justices' decision to grant Kjoller's petition.

"This is what other judicial entities should be doing in response to the very serious problems of hallucinations coming from these legal research [large-language models]," he said.

Scheck said the legal profession needs to grapple with the risks AI use poses. He noted that the professors' amicus letter cited a recent Stanford study that analyzed the hallucination rates of LLMs in response to legal queries and found that OpenAI Inc.'s ChatGPT 4 hallucinated 58% of the time and Meta Platform Inc.'s Llama 2 hallucinated 88% of the time. Even LLMs that specialize in law, developed by LexisNexis and Thomson Reuters, have been found to hallucinate between 17% and 33% of the time, according to the letter.

"When you have vendors like those cited in the Stanford study having such high hallucinations rates, that's a serious problem, and we haven't begun to deal with it," Scheck said.

Scheck added that according to the professional legal ethics rules, it's the responsibility of lawyers in supervisory positions to ensure that other lawyers don't repeat errors in legal briefs, and that starts with an understanding of AI tools' risks and vendors providing the services.

"There are a lot of these cases," Scheck said. "They involve all kinds of lawyers in all kinds of disciplines, but when you have a district attorney doing this, it is especially troubling."

The amici law professors are represented by Vasudha Talla of Emery Celli Brinckerhoff Abady Ward & Maazel LLP.

Kjoller is represented by Carson White, Katherine Claire Hubbard and Salil Hari Dudani of the Civil Rights Corps, and Thomas Angell of the Nevada County Public Defender's Office.

The real party of interest is Nevada County District Attorney Jesse Wilson.

The case is Kyle Kjoller v. Superior Court of Nevada County, case number S293723, in the California Supreme Court.

--Editing by Robert Rudinger.

*Law360 is owned by LexisNexis Legal & Professional, a RELX company.*

# Conn. Judges Add 'No-Tolerance' AI Warnings To New Dockets

By **Emily Sawicki**

Law360 (September 24, 2025, 12:07 PM EDT) -- Federal judges in Connecticut have begun entering warnings on new case dockets notifying litigants and their counsel of a "no-tolerance policy" when it comes to briefs that include hallucinated arguments and citations, regardless of whether artificial intelligence was used.

The policy, which is also available through **a notice** posted on the District of Connecticut's website, warns that "attorneys and pro se litigants alike should exercise great caution in submitting any AI-generated language in filings before the court." The notices appear to be included on the docket of all new cases filed in the district, with the first added to the docket late last week.

The notice comes as dozens of federal judges in districts from Hawaii to New Jersey have **issued standing orders** relating to the use of AI in their courts, dating back to 2023. The District of Connecticut cites one such **standing order**, issued in May by U.S. Magistrate Judge David L. Horan of the Northern District of Texas, in its notice.

Both Judge Horan's standing order and the new Connecticut notice reference Rule 11 of the Federal Rules of Civil Procedure, which governs how attorneys or pro se parties may draft and file documents, and imposes sanctions for filings that fall short.

"Use of AI without verification of the accuracy of the information it generates — like any other shoddy research method from other sources or tools — implicates Federal Rule of Civil Procedure 11, the central purpose of which is to deter baseless filings in district court and thus to streamline the administration and procedure of the federal courts," the District of Connecticut notice stated. It added, "Rule 11 applies fully to actions filed by pro se litigants."

The District of Connecticut "has a no-tolerance policy for any briefing (AI-assisted or not) that hallucinates legal propositions or otherwise severely misstates the law," the notice stated, warning that such errors "will often result in sanctions absent reasonable excuse."

Courts have begun imposing **increasingly stringent** sanctions for filings that include AI-generated errors. In recent months, some judges have found that botched use of AI **violates Rule 11**, while others have turned to their **inherent authority** to issue sanctions.

--Editing by Robert Rudinger.

# His Client Got A Pro Se Suit. Then The AI Filings Started.

By **Chris Villani**

Law360 (January 5, 2026, 10:40 AM EST) -- At first, a pro se suit filed against one of Kraig Long's clients looked like any other employment case. The complaint brought by a Washington, D.C., worker was filed in a far-flung Virginia state court district.

"There was not much in there, and we thought it was a weak case," said Long, a partner at Nelson Mullins Riley & Scarborough LLP.

But once Long responded to the complaint, he and his client were hit with a flurry of motions — 21 in total — sometimes coming at a clip of nearly one per day.

The pro se plaintiff was using artificial intelligence to draft his barrage of challenges, something that employment attorneys say is becoming increasingly more common, with the potential to clog up dockets, drag out cases, and make litigation significantly more expensive.

"We are absolutely seeing an uptick in AI use by pro se litigants," said Eric Felsberg, the leader of Jackson Lewis PC's subgroups for AI governance and bias testing and pre-employment assessments.

"I won't say it's easy to spot, but there are definitely signs you can pick up on," Felsberg said. "You'll see very polished submissions. The papers will bring up good, solid, legal arguments that pick up on complexities that you would not expect to see in a pro se submission."

While AI has been touted as a way to provide access to the courts for individuals who might otherwise be mystified by navigating the legal system without a lawyer, not all attorneys welcome the trend.

"Not only are there more lawsuits, but they are harder to kick," said Sal Simao, another Nelson Mullins employment attorney who practices in New York and New Jersey.

"Are they winning lawsuits? Probably not. But we are seeing people file appeals to the Third Circuit because the AI tells them how to do it," Simao said. "It's becoming harder and harder to budget, because you don't know what's going to happen. It's not a normal case."

## "He Kept Us on Our Heels"

For weeks, Long and his team navigated the onslaught of motions, which included a motion to strike their answer to the complaint, a motion to prevent them from being admitted pro hac vice in Virginia, and motions for reconsideration if the first attempt were denied by the judge.

"I'll be honest, they were well-written," Long said. "They were presumably citing good law, and we had to respond to them day after day after day after day. The guy kept us on our heels for the first three months of the case."

Howie Wexler, a labor and employment lawyer with Seyfarth Shaw LLP, said he first encountered a pro se plaintiff using AI last year when helping a client try to resolve a charge with the U.S. Equal Employment Opportunity Commission. Since then, he said, the use of AI by pro se plaintiffs has "increased tenfold."

Felsberg said the use of AI is "empowering pro se plaintiffs" and can sometimes be helpful to defense attorneys because filings are easier to understand than they would be in most pro se matters.

"Before, if you got a complaint, it may be, for lack of a better description, kind of a rambling statement," he said. "We'd have to ask: 'Is a claim even asserted here? What violation of the law are they claiming?'"

But while AI can streamline a pleading and make it easier to read for an attorney, it isn't always helpful, even for the plaintiffs using it. Some of the well-worn AI pitfalls like hallucinations can permeate filings, a trap experienced attorneys have occasionally fallen into in various types of cases.

Wexler stressed the need to check every single case citation in pro se matters to make sure the cases being relied upon are indeed real.

"That was not something that was a concern several years ago," he said. "But I have seen it more in the past six months than I had in 20 years of practicing law."

Kellen Safreed, a plaintiff-side employment attorney with Sherin and Lodgen in Boston, said he often sees potential clients come in with AI-aided pleadings information that is "true, but irrelevant."

"They will bring a summary that includes citations or statutes or cases out of Indiana," Safreed said. "Maybe that's a real thing, but it has nothing to do with their Massachusetts employment claim."

AI also has a tendency to tell the user what the user wants to hear, Safreed added.

"Someone wants to quit their job, but they want to get severance, and AI says, 'Sure, it's called constructive discharge,'" he said. "They get their hopes up, but they don't realize that is a really high bar. Your boss being miserable to the point where you want to quit your job is probably not going to be a constructive discharge claim."

Simao said AI is making it harder to know whether a document is real, citing a recent case in which a pro se plaintiff created a picture and audio recording to support their case and a notarized document that his Nelson Mullins team thought was real.

"We took the extra step of calling the notary, who couldn't remember but checked her log and then told us it was a forged document," he said. "While authenticating evidence is always an issue, pro se plaintiffs tend to be treated more leniently by courts, and forgeries are getting harder to detect."

### **ChatGPT-Client Privilege?**

The use of AI can also invite complicated questions around privilege. Safreed said there is "huge uncertainty" about where and when attorney-client privilege would apply when AI is involved.

"If a client uses AI to summarize their claims, is the record that exists of that exchange privileged? I don't know," he said. "I think that's an open question."

A company defending a claim could potentially file a motion seeking to compel production of the ChatGPT prompts from a server, he said.

"I think employees should be cautious about that," Safreed added.

Seyfarth's Wexler envisioned the possibility of a whole new category of evidence that litigants are going to want to get their hands on, related to communications between a person and a public AI platform.

"There is a potential treasure trove of information," he said.

In Long's Virginia case, he said that the plaintiff — who made no secret of the fact he was using AI to help advance his case — may have repeatedly entered different potential claims into ChatGPT to see which one had the best chance to stick. His colleague, Simao, said that is common among pro se plaintiffs.

"Basically, if they went to an attorney, the attorney would say, 'You don't have a claim,'" Simao said. "If you chat on one of the OpenAI systems and say you are having an issue at work, you can ask, 'What can I sue for?' The AI will make a claim for them. If they don't have the facts, they will get the facts."

Experts said it's important for attorneys to protect their own privileged information while dealing with a pro se plaintiff using AI. Long advised trying to obtain a protective order early on in the case to bar the plaintiff from running a client's documents through an AI platform, something he said happened in the Virginia lawsuit.

### **A Loss for Everyone**

Ultimately, when it came time to deal with matters in person, Long's experience won the day. The plaintiff showed up for a deposition with a friend of his toting an old-school video camera and tried to record the deposition without a court reporter, something that was not allowed in the southern Virginia state court and was shut down by the judge.

By the time the plaintiff was able to get a court reporter, the discovery clock had run out. Long said the plaintiff struggled during a dispositive motion hearing, even though his written responses to their filings had been fairly strong.

"ChatGPT couldn't help him at the hearing," Long said.

Long, who gave a seminar to his colleagues detailing his experience, said the use of AI in this case was probably bad for everyone. Although he won a summary judgment motion for his client, the case was much longer and more expensive than it otherwise would have been. Long also said AI made the plaintiff believe his case was stronger than it actually was, which prevented a settlement.

"We made some very reasonable offers, and he just turned his nose up and said 'no,'" Long said.

He said there needs to be additional rulemaking or possibly legislation governing the use of AI in legal filings. He also predicted that judges, who are typically lenient when it comes to pro se plaintiffs, might become stricter if their dockets are jammed up by meritless cases that drag out through extensive motion practice.

"If you have a meritorious claim, AI serves a good purpose for those who cannot afford counsel, and lawyers are not getting cheaper," Long said. "But it also empowers those with frivolous cases to take them further than they thought. Unchecked, it's going to create serious issues for our courts."

Safreed said he could understand why individuals would turn to AI, despite its pitfalls, if they felt they had a lawsuit to bring.

"A company that gets sued all the time, they know exactly what to do. But I deal largely with people who have never had to engage an attorney before and, hopefully, never will again," he said. "Often, they are perfectly reasonable people who are unfamiliar with the legal machinery. That invites the usage of AI."

--Editing by Robert Rudinger.

A hand in a dark suit jacket is shaking a metallic, robotic hand. The background is a wall covered in faint, golden circuitry and text. In the foreground, there are stacks of books on the left and a stack of papers on the right. The lighting is dramatic, with a strong light source from the right, casting long shadows.

ARDC

ATTORNEY REGISTRATION &  
DISCIPLINARY COMMISSION

# THE ILLINOIS ATTORNEY'S GUIDE TO IMPLEMENTING AI

ADDISON  
WESLEY



## MESSAGE FROM THE ADMINISTRATOR

As lawyers, we are living in a time of rapid change. Few innovations are reshaping our profession as quickly as artificial intelligence. While these tools hold promise to make our work more efficient and accessible, they also raise new questions about privacy, security, confidentiality, and the exercise of professional judgment. These are not the only considerations, but they are among the most important when it comes to protecting our clients, maintaining trust, and ensuring our work meets the highest standards of the profession.

The ARDC developed this guide to serve as a resource for Illinois lawyers who want to understand and implement AI responsibly in their practices. Designed with solo and small firm practitioners in mind (who may not have the IT support available in larger firms) the information here is useful for lawyers and firms of every size.

This guide complements the Illinois Supreme Court's Policy on Artificial Intelligence and judicial reference sheet. While the Court's policy sets the foundation, this guide focuses on the practical side—helping firms of all sizes apply that framework in daily practice. It includes detailed explanations of how AI systems work. Even if those parts feel technical, they are included so that every lawyer (especially those without dedicated IT staff) has the practical understanding needed to use AI tools safely and ethically.

Our goal is to support you in navigating these changes with confidence. Along with sample policies, forms, and a step-by-step framework, this guide is intended to help you evaluate AI tools, protect client data, and communicate openly with those you serve. No matter the size of your practice or where you are on this journey, you are not alone—ARDC is here as a resource and partner every step of the way.

With respect and support,

*Lea S. Gutierrez*

# The Illinois Attorney's Guide to Implementing AI

---

Prepared by the Illinois Attorney Registration and Disciplinary Commission (ARDC)<sup>1</sup>  
Effective Date: *October 1, 2025*

## Contents

Introduction.....	3
Illinois Supreme Court Policy on Artificial Intelligence .....	3
The Core Framework.....	5
What is Generative AI? .....	5
Side Note: Generative Versus Extractive AI.....	6
Key Takeaways .....	7
How to Choose an Appropriate GAI Tool.....	7
Step 1: Classify the Information to Be Processed.....	7
Step 2: Categorize the GAI Tool.....	9
Step 3: Evaluate and Document the Applicable GAI Safeguards .....	12
Managing Client Rights.....	18
Key Takeaways .....	21
Implementing the Practice Resource Kit.....	22
GAI Terms of Use Checklist.....	22
Sample Notice of Artificial Intelligence Practices.....	22
Sample Use of GAI Tools Policy.....	22
Sample Informed Client Consent Form.....	23
The Road Ahead .....	23
Technical Addendum .....	25
Model Training .....	25
Conversation and Document Storage.....	27
Retrieval-Augmented Generation.....	28
Data Retention Within the Model .....	28

---

<sup>1</sup> The primary author of this Guide is Aaron W. Brooks, who contracts with ARDC to serve as its Chief Information Security Officer and primary legal and technical advisor on artificial intelligence. Mr. Brooks is also the Chair of ISBA's Steering Committee on Artificial Intelligence.

Data Retention for Abuse Monitoring .....	29
Data Isolation .....	29
Supporting Resources and Materials .....	31
Appendix 1 Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI.....	32
Appendix 2 GAI Terms of Use Checklist.....	37
Appendix 3 Sample Notice of Artificial Intelligence Practices.....	38
Appendix 4 Sample Use of GAI Tools Policy .....	41
Appendix 5 Sample Informed Client Consent Form.....	46
Appendix 6 Cybersecurity Information Sheet (“CIS”) Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems .....	48

## Introduction

The Illinois Attorney Registration and Disciplinary Commission (“ARDC”) has completed a careful study of Generative Artificial Intelligence (“GAI”) and is pleased to provide this guidance to assist Illinois attorneys in understanding, adopting, and using GAI responsibly. This Guide should be read in conjunction with the Illinois Supreme Court Policy on Artificial Intelligence.<sup>2</sup> If any portion of this Guide is deemed to be inconsistent, the Court’s Policy controls.

We recognize artificial intelligence as a transformational technology that, when used carefully, has the potential to streamline legal services, expand access to justice for clients across Illinois, and generally strengthen our profession for many years to come. This Guide is designed to equip lawyers with a foundational understanding of how Generative Artificial Intelligence systems function, what risks they may pose, and how they can be integrated into legal practice ethically and effectively.

Included with this Guide is a Practice Resource Kit that lawyers might consider as a means to help implement GAI tools into their practice. The Practice Resource Kit contains samples, templates, and checklists, including: A sample client notice, a sample staff policy, a sample informed consent form, and a checklist for reviewing GAI terms of service. Lawyers using these resources should do so very carefully to ensure that the language finally used fits the particular situation for which they are implemented. It is not our intent to establish practice standards. These resources are nonbinding, and not Court policy.

## Illinois Supreme Court Policy on Artificial Intelligence

On December 18, 2024, the Illinois Supreme Court announced a new Policy on Artificial Intelligence, together with a judicial reference sheet on AI, both of which we reproduce at Appendix 1.<sup>3</sup> We believe the Policy provides a clear foundation for lawyers’ responsible use of GAI. It affirms that attorneys may use AI tools, provided they do so in accordance with existing professional obligations.<sup>4</sup> Specifically, the Policy makes four key points:

GAI Use is Authorized. The Policy authorizes the use of artificial intelligence by attorneys, subject to the requirements set forth in the Policy.<sup>5</sup> For those who choose to incorporate one or more GAI tools into their practice, ARDC is fully committed to staying focused on the benefits and risks associated with GAI and providing resources to help them implement GAI in a safe and responsible manner.

Attorney Accountability. Attorneys who use artificial intelligence in their practice must thoroughly review and assume professional responsibility for any AI-generated information that is incorporated into their work

---

<sup>2</sup> Ill. Sup. Ct., *Policy on Artificial Intelligence* (effective Jan. 1, 2025), reproduced in App. 1.

<sup>3</sup> *Illinois Supreme Court Announces Policy on Artificial Intelligence*, Illinois Courts (Dec. 18, 2024), <https://www.illinoiscourts.gov/News/1485/Illinois-Supreme-Court-Announces-Policy-on-Artificial-Intelligence/news-detail> (last accessed Oct. 9, 2025).

<sup>4</sup> *Policy on Artificial Intelligence*, *supra* note 2.

<sup>5</sup> *Id.* (“The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards.”).

product.<sup>6</sup> ARDC maintains a PMBR Self-Assessment program that provides several tips and resources to help manage this core duty.<sup>7</sup> We will continue to provide educational resources to help attorneys apply the Illinois Rules of Professional Conduct to GAI.

Duty of Competence. The Policy requires attorneys who use artificial intelligence tools to understand those tools and ensure that they are secure and legally compliant.<sup>8</sup> This aspect of the Policy echoes the long-standing rule set forth in Illinois Rule of Professional Conduct 1.1 that an attorney’s duty of competence extends to the benefits and risks associated with technology.<sup>9</sup>

Privacy and Security. The Policy requires attorneys to confirm that GAI tools maintain the privacy and security of confidential and personally identifiable information. Specifically, the Policy states:

*“The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.”<sup>10</sup>*

This component of the Policy corresponds to a lawyer’s duty to preserve client confidentiality, including the security of any client data in the lawyer’s possession.<sup>11</sup> Determining whether a GAI tool is appropriate for handling this type of information can be complex. For that reason, this aspect of the Policy was a central focus in drafting this Guide. We have included policies, checklists, and practical examples to support attorneys in evaluating and implementing GAI tools in a manner that protects sensitive data and complies with legal and ethical obligations.

Accountability, competence, and confidentiality form the essence of a professional and ethical approach to using artificial intelligence in the practice of law. The Court’s Policy serves as a clear signal that, while the

---

<sup>6</sup> *Id.* (“The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations.”).

<sup>7</sup> Ill. Att’y Registration & Disciplinary Comm’n, *Artificial Intelligence: Benefits, Risks, and Ethical Considerations* (2024), <https://pathlms.iardc.org/courses/69187/sections/76987> (last visited June 21, 2025).

<sup>8</sup> *Policy on Artificial Intelligence*, *supra* note 2 (“Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.”).

<sup>9</sup> Ill. R. Prof’l Conduct R. 1.1 cmt. 8 (2023) (“To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”).

<sup>10</sup> *Policy on Artificial Intelligence*, *supra* note 2.

<sup>11</sup> Ill. R. Prof’l Conduct R. 1.6 cmt. 18 (2025) (“Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.”).

Illinois Supreme Court supports the use of GAI, it expects lawyers to exercise judgment, maintain control over their work, and uphold their ethical obligations at every step.

## The Core Framework

### What is Generative AI?

On June 12, 2017, researchers from Google and the University of Toronto released a groundbreaking paper titled *Attention Is All You Need*, introducing a new type of technology called a *transformer*.<sup>12</sup> This breakthrough is widely regarded as the watershed moment for modern artificial intelligence, and it forms the technological foundation for nearly all AI systems that lawyers are likely to encounter in their daily workflow.<sup>13</sup>

Soon after *Attention Is All You Need* was published, researchers from OpenAI demonstrated that the new transformer technology could be configured to understand and mimic natural human language.<sup>14</sup> They did this using machine learning techniques now commonly referred to as "*model training*" and "*fine-tuning*."<sup>15</sup> Later in this Guide, we will discuss how model training might threaten client confidentiality and what lawyers should do to mitigate this risk.

These core research efforts formed the basis of what is now commonly known as Generative Artificial Intelligence. The family of GAI tools includes two variations that frequently arise in the practice of law:

- *Large Language Models*, or "*LLMs*", which can quickly generate, interpret, and summarize human language in response to prompts;<sup>16</sup> and
- *Vision Models*, which can generate realistic images and video from basic descriptions or examples, and are often the subject of legal discourse regarding deepfake fraud and evidentiary manipulation.<sup>17</sup>

The term "model" is a very important concept for understanding GAI, because the data processing behind most AI-enabled applications (including tools marketed to the legal industry) is typically performed by one of a few central companies that specialize in building, training, and licensing GAI models.<sup>18</sup> These companies

---

<sup>12</sup> Ashish Vaswani et al., *Attention Is All You Need*, in *Advances in Neural Information Processing Systems 30* 6000 (I. Guyon et al. eds., 2017) (paper presented at the 31<sup>st</sup> Int'l Conf. on Neural Info. Processing Sys. (NIPS '17)).

<sup>13</sup> John Berryman & Albert Ziegler, *Prompt Engineering for LLMs* (O'Reilly Media, Inc. 2024).

<sup>14</sup> Alec Radford et al., *Improving Language Understanding by Generative Pre-Training* (OpenAI 2018).

<sup>15</sup> Numa Dhamani & Maggie Engler, *Introduction to Generative AI* (Manning Publications 2024).

<sup>16</sup> Edward Raff et al., *How Large Language Models Work* (Manning Publications 2025).

<sup>17</sup> ARDC does not currently recognize a universal term of art for image and video generation models. The term "Vision Models" is used in this Guide in a representative capacity to cover a range of technologies, including diffusion models, vision transformers, and other generative image architectures. For a useful discussion of this area, see Amit Bahree, *Generative AI in Action* (Manning Publications 2023).

<sup>18</sup> Suhas Pai, *Designing Large Language Model Applications* (O'Reilly Media 2025) (explaining the broad landscape of models and model providers in Chapter 5).

maintain and update the underlying model architecture, while legal technology vendors integrate those models into products designed for lawyers.

One analogy we find helpful is that of *makes* and *models* in the automotive industry. Automobiles are generally classified by their make, model, and sometimes a trim or body style. For example, Honda (the *make*) produces the Accord (the *model*) which comes in different versions with varying features.<sup>19</sup> GAI producers and their models can likewise be conceptualized this way, as depicted in Table 1 below.

Core Company	Transformer Model	Native Model Platform
OpenAI and Microsoft	GPT	ChatGPT and Copilot
Anthropic	Claude	Claude.ai
Google	Gemini	Gemini
Meta	Llama	MetaAI

**Table 1: Table showing major GAI companies, models, and core applications**

As you can see, many model producers use their own model to power a native application that is licensed directly by that provider. For example, OpenAI provides the “GPT” branded model for third parties to integrate into their applications, but OpenAI also uses that same model to directly provide various versions of ChatGPT.<sup>20</sup>

#### Side Note: Generative Versus Extractive AI

Throughout this Guide, we use the term *generative* to refer to the core architecture that underlies almost every modern artificial intelligence application used within the practice of law. The transformer is considered *generative* because it is designed to produce outputs in response to inputs. In some cases, those outputs take the form of new content (such as text or images); in other cases, the outputs may be reformulated queries or summaries that retrieve material from an external data source. However, you may encounter AI discussions that divide AI systems into two basic types: *generative* and *extractive*. We do not view this as a significant distinction, because the terms *generative* and *extractive* are simply descriptions of two functions that the same underlying transformer model might be used to produce.<sup>21</sup> Accordingly, when the terms *Generative Artificial Intelligence* and *GAI* are used throughout this Guide, we mean for those terms to encompass systems which perform both *generative* and *extractive* functions. In short, it’s important for lawyers to understand the basic GAI risk assessment that applies to all GAI tools, whether they are acting in a *generative* or *extractive* capacity.

---

<sup>19</sup> *Honda Accord Family, Sedans and Hybrids*, Honda, <https://automobiles.honda.com/accord> (last visited Sept. 11, 2025).

<sup>20</sup> See, e.g., Schellman & Co., LLC, *Independent Service Auditor’s SOC 3 Report for the API and ChatGPT Business Product Services System for the Period of January 1, 2025 to June 30, 2025* (Aug. 7, 2025), <https://trust.openai.com>.

<sup>21</sup> See, Andrew Freed et al., *Effective Conversational AI: Chatbots that Work* (Manning Publications 2025) (explaining that, historically, “extractive” AI referred to classifier-based systems, but modern transformer-based systems can perform both extractive and generative functions within the same architecture); See also, Trey Grainger et al., *AI-Powered Search* (O’Reilly Media 2025) (describing how GAI models are used in various search contexts, including extractive, abstractive, and generative search modes).

## Key Takeaways

Taking all this together, the key things you should understand from this section are:

- When artificial intelligence is used within the practice of law, it is almost universally focused on the 2017 technology breakthrough called a *transformer*, which is the foundation for Generative Artificial Intelligence.
- Transformers can be understood using a “*make and model*” analogy, whereby AI-focused companies (such as OpenAI and Anthropic) produce various transformer models (such as GPT and Claude).

When lawyers consider whether a particular GAI tool is appropriate for processing various types of information (including confidential or sensitive client information), it’s important to understand that this information is being transmitted to, and processed inside, a particular transformer model. Thus, lawyers should know who produces that model, and what privacy and security safeguards are in place.

With that basic understanding in place, let’s move ahead to the next section, in which we apply this knowledge to build a framework lawyers might use to evaluate various GAI tools for use in their practice.

## How to Choose an Appropriate GAI Tool

Lawyers do not need to become AI experts to use GAI tools effectively, but they do need a structured approach to evaluating the many tools that are available, classifying the type of data these tools will process, and communicating with clients about how GAI may be used to work on their matters.

This section outlines a practical, step-by-step framework that can be adapted to most practice settings. We do not intend this to be mandatory, but we encourage lawyers to adapt this framework to their own practices. The framework is offered as a nonbinding example which, if adapted to a lawyer’s specific circumstances, may help document the safeguards required under Illinois Rule 1.6 and support a showing of reasonableness.

### Step 1: Classify the Information to Be Processed

It should be clear at this point that not every GAI tool on the market is appropriate for every type of data lawyers may wish to process. Therefore, when selecting a GAI tool, lawyers must first clarify what information they intend to use that system to process. We suggest the following classifications, presented in order of lowest to highest risk:

#### (a) General Information

If information is entirely unrelated to any matter the lawyer has undertaken professionally, and is otherwise not subject to any confidentiality protections, we consider it “General Information” and assign the lowest level of risk. Examples include using GAI tools for internal technology troubleshooting, generating forms and checklists, drafting marketing content or assisting in writing blog articles.

## (b) De-Identified Information

If information relates to the representation of a client, but there is no reasonable likelihood that it could be used to ascertain the identity of the client or matter, we classify this as “*De-Identified Information*.” This includes true hypotheticals and other scenarios that satisfy Rule 1.6, Comment [4], which permits discussion so long as the listener could not reasonably identify the client or matter.<sup>22</sup>

When evaluating whether there is a reasonable likelihood that information could be used to ascertain the identity of a client or matter, lawyers should bear in mind that artificial intelligence systems are exceptionally good at detecting patterns and correlations that may allow reidentification of information that appears anonymous to a human.<sup>23</sup> Accordingly, lawyers are encouraged to consider more formal methods of creating De-Identified Information, particularly in sensitive matters.<sup>24</sup> This concern extends beyond direct data entry into GAI tools, because these systems are frequently trained on data scraped from the internet. Similar re-identification risks can arise when lawyers post hypotheticals or case summaries in public forums, blogs, or listservs.

In short, while De-Identified Information carries less risk than identifiable client information, it is not risk-free and should still be managed appropriately when processed by a GAI tool.

## (c) Confidential Information

For purposes of this Guide, “*Confidential Information*” means information that is protected by Rule 1.6, or is otherwise subject to confidentiality obligations, but does not contain Sensitive Personal Information as defined below. Confidential Information includes information that relates to the representation of a client that could reasonably be used to identify the client or the situation involved, even if direct identifiers are omitted.

## (d) Sensitive Personal Information

For purposes of this Guide, we believe that some types of Confidential Information merit additional protection. In our view, Illinois public policy calls for information that is specifically listed in the Illinois Personal Information Protection Act to be granted additional safeguards.<sup>25</sup> This includes:

- Social Security numbers and tax returns
- Driver’s license numbers or state identification card numbers
- Account, credit card, or debit card numbers
- Medical information, including mental health and substance abuse treatment records
- Health insurance information

---

<sup>22</sup> Ill. R. Prof’l Conduct R. 1.6 cmt. 4 (2025).

<sup>23</sup> John X. Morris et al., *DIRI: Adversarial Patient Reidentification with Large Language Models for Evaluating Clinical Text Anonymization*, AMIA Jt. Summits Transl. Sci. Proc. (2025).

<sup>24</sup> See, e.g., U.S. Dep’t of Health & Human Servs., *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012).

<sup>25</sup> 815 ILCS 530/5.

- Unique biometric identifiers or biometric information (as defined in Illinois law)
- Passwords and security question/answer pairs
- Any other information meeting PIPA’s definition of “personal information,” even if separated from a first name or first initial in combination with last name

Whether a lawyer may be required to take additional steps to comply with other laws, such as state and federal laws that govern data privacy, is beyond the scope of this Guide.

## Step 2: Categorize the GAI Tool

For purposes of this Guide, we group GAI tools into two main categories: Third-party managed, and self-managed. Each category has distinct implications for confidentiality, security, and client communication. This section describes these broad categories and explains how best to classify any given GAI tool.

### (a) Third-Party Managed GAI Tools

A GAI tool is “*third-party managed*” if the essential components of the tool are under the direct control of someone other than the lawyer or the law firm. When a lawyer transmits data to such a GAI tool for storage and processing, that data too becomes within the direct control of the third-party. Architecturally, this hosting and management structure is similar to other cloud-based systems that a lawyer may already use. Nevertheless, these tools introduce unique data processing techniques that are new to the world of cloud-based systems. Accordingly, GAI tools present unique risks above and beyond those associated with traditional cloud systems.

In some descriptions, a GAI tool may be referred to as a “*public*” tool. For purposes of this Guide only, “*public*” means a GAI tool that: (i) is operated and controlled by an entity other than the lawyer or law firm; and (ii) strongly aligns with the public category (discussed further below and illustrated in Table 2). As an illustration, and without endorsing any particular vendor, tools such as ChatGPT have some versions which are public, some that are licensed under consumer-oriented terms of service, and other versions which are licensed under business-class terms of service.<sup>26</sup> This terminology is used solely for the purposes of this Guide and does not constitute legal advice or state the views of the Illinois Supreme Court.

In Step 3 of this section, we outline the main safeguards that should be considered when evaluating third-party managed GAI tools. Before we do that, however, you should clearly understand the difference between two types of third-party managed GAI tools: Native Model Platforms and API Integrations. This distinction matters, because Step 3 applies differently depending on which type of third-party managed tool is being evaluated.

For example, in the case of a Native Model Platform, issues such as model training are addressed directly in the platform’s Terms of Use. By contrast, when using an application that integrates with a model provider, the lawyer is not directly involved in selecting the underlying model, and additional research may be necessary to confirm whether appropriate safeguards are in place.

---

<sup>26</sup> As of the Effective Date of this Guide, the free version of ChatGPT is a “public” tool, while the ChatGPT Plus and Pro versions are consumer-aligned tools.

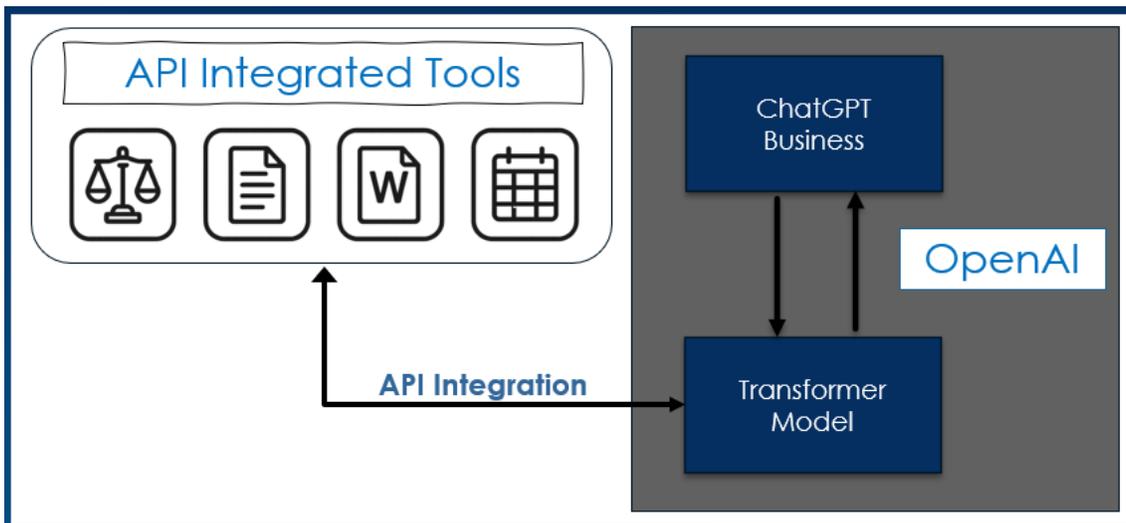
## (1) Native Model Platforms

In a Native Model Platform, all AI processing occurs on infrastructure operated by the model provider itself. Examples include ChatGPT (built and hosted by OpenAI), Claude (built and hosted by Anthropic), and Gemini (built and hosted by Google). The same company (together with subprocessors engaged directly by this company) controls both the transformer model and the hosting environment that stores, transmits, and processes data. Accordingly, a Native Model Platform presents a security tradeoff: Users don't have direct control over how their data is stored and processed, but users also don't have direct responsibility for managing the underlying performance and security of the system. Native Model Platforms may be a practical option for some lawyers if they include safeguards that are appropriate for the type of information being processed.

One variation of this idea is an “*enterprise-walled environment*” whereby a third party is still fully managing the transformer model and the underlying infrastructure that stores and processes data; however, unlike multi-tenant systems like ChatGPT, Claude, and Gemini, the environment is more isolated and controlled by the user. Systems that are set up within the Microsoft Azure OpenAI infrastructure (discussed more in the Data Isolation sections in Step 3 and the Technical Addendum) are good examples of what we mean by “*enterprise-walled environments*.” As with Native Model Platforms, enterprise-walled environments present a security tradeoff: Users have more direct control over how their data is stored and processed, but users also take on greater responsibility for managing and maintaining the performance and security of the system.

## (2) API Integrations

As depicted below, API integrated applications are typically built using the same underlying infrastructure as Native Model Platforms. Many services with GAI functionality use the same underlying models and model providers to process data.<sup>27</sup>



**Figure 1: Conceptual illustration of data being sent from various GAI tools to an OpenAI transformer model via API integration.**

<sup>27</sup> Schellman, *supra* note 20 (showing that the ChatGPT Enterprise Layer and third-party API users access the same cloud infrastructure).

Any software provider can add AI functionality to their application using a transmission channel called an *Application Programming Interface*, or *API*. When developers connect their software to a model provider's API, they create a two-way communication between your data and one or more underlying transformer model providers (such as OpenAI, Anthropic, or Google).

Distinguishing between the underlying model and the products that integrate these models is important. Lawyers often interact with GAI tools through branded interfaces, but the actual transformer model is typically managed directly by the underlying model provider. For example, consider a PDF application that has an AI feature allowing you to summarize PDF documents. Behind the scenes, that feature most likely works as follows:

- User clicks "Summarize Document"
- The PDF application sends the document content to a model provider (such as OpenAI) using that model provider's API interface
- The model provider processes the document with their transformer model, and sends a summary back to the PDF application
- The PDF application then displays the transformer model's output to the user

Although the user interacts directly with the application, the underlying AI processing occurs on infrastructure controlled by the model provider and is subject to whatever privacy and security assurances are negotiated between the application provider and the model provider. In short, applications with AI integrations may give the appearance of operating in an isolated environment, but this is rarely the case. In most cases, these arrangements simply shift the relationship with the transformer model provider from that of your direct vendor to that of your vendor's subprocessor.

When attorneys evaluate whether a particular GAI tool is suitable for use in their practice, it's essential for them to investigate what model is used to create the artificial intelligence experience. A reputable legal services provider should be transparent about the model vendors they use, and they should make that information readily available to lawyers prior to licensing the product. For example, and without endorsing any specific provider, at the time of this writing Thomson Reuters publicly states of its CoCounsel product: "We process all interactions with OpenAI GPT and Google Gemini in the U.S."<sup>28</sup>

### (b) Self-Managed GAI Tools

In a self-hosted environment, the transformer model is downloaded and deployed directly onto hardware or cloud infrastructure controlled by the user. This includes models such as GPT-OSS, Mistral, or Llama, which can be run entirely within a firm's own servers or secure virtual environments, and in some cases directly on a lawyer's own computer. Self-hosted models offer the highest level of control over data storage, processing, and retention, since no information is likely to be transmitted to any third party.

---

<sup>28</sup> *CoCounsel: The Industry-Leading GenAI Assistant for Professionals*, Thomson Reuters, <https://www.thomsonreuters.com/en/cocounsel> (last visited Oct. 4, 2025).

Self-hosting an AI model provides the greatest degree of control over data handling and system configuration, but it also carries the highest level of technical complexity and security responsibility. Although Step 3 below includes the main GAI safeguards associated with self-hosted models, lawyers who choose to go this route might consider working with qualified technical support to ensure their implementation is supported by a well-documented risk management plan.

### Step 3: Evaluate and Document the Applicable GAI Safeguards

At this point in the evaluation process, a lawyer should clearly understand the level of data sensitivity a GAI tool will be used to process, as well as the structural category within which the GAI tool falls. Next, the lawyer should apply the applicable GAI tool safeguards provided in this Step 3 to confirm that the tool is appropriate for the type of data it will be used to process.

Rule 1.6 of the Illinois Rules of Professional Conduct (“*Confidentiality of Information*”) is helpful on this point. Specifically, Committee Comment [18] of Rule 1.6 lists five non-exclusive factors that lawyers should evaluate to determine the reasonableness of their efforts to prevent inadvertent or unauthorized disclosure of client confidential information:

1. The sensitivity of the information;
2. the likelihood of disclosure if additional safeguards are not employed;
3. the cost of employing additional safeguards;
4. the difficulty of implementing the safeguards; and
5. the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Accordingly, as the sensitivity of the data increases, more GAI tool safeguards must be present to make a showing of reasonableness. This is particularly true where the additional safeguards do not create significant additional costs, implementation difficulty, or adverse impacts upon the lawyer’s representation.

#### (a) Third-Party Managed GAI Safeguards

This section describes the main categories of privacy, security, and compliance safeguards to consider when evaluating third-party managed GAI tools, including both Native Model Platforms and API integrations. In the next section, we’ll cover the safeguards to consider with self-managed GAI tools.

In Table 2 below, we identify the main risks associated with third-party managed GAI tools and show how those risks are typically addressed at different levels of privacy and security. Some of these safeguards are new and unique to artificial intelligence (such as not allowing Confidential Information or Sensitive Personal Information to be used in training models) while others are long-standing concerns in any cloud-based service. Yet, because GAI tools can process, store, and potentially reuse information in unique ways, even traditional risks can take new forms and deserve renewed scrutiny. Additionally, considering that GAI capabilities are becoming embedded into most technology systems attorneys already use, the approach outlined in this Guide should be applied broadly to most systems that store or process client data, even those which are not obviously “*artificial intelligence*” applications.

We divide third-party managed tools into four broad categories (public, consumer, business, and enterprise), but we acknowledge that specific GAI tools may not fit neatly within one category. The takeaway is that tools aligned with public and consumer-aligned safeguards are less likely to be appropriate for processing confidential or sensitive personal information, and tools aligned with the business or enterprise safeguards are preferable.

GAI Safeguard	Public	Consumer	Business	Enterprise
<b>Authentication</b> User identity verification and access control mechanisms	Open	Basic	Secure	SSO
<b>Model Training</b> Use of customer data to improve current and future models	Required	Opt-Out	Prohibited	Prohibited
<b>Data Retention</b> User data storage, retention policies, and deletion procedures	Perpetual	Platform-Defined	User-Defined	Admin-Defined
<b>Data Isolation</b> Separation and protection of customer data and workloads	Undefined	Noncommittal	Logical Separation	Dedicated
<b>Supply Chain Risk</b> Third-party dependencies, vendor security, and supply chain integrity	Undefined	Noncommittal	Transparent	Regulated
<b>AI Risk Management</b> AI governance, safety controls, and responsible AI practices	Undefined	Noncommittal	Industry-Standard	Framework-Based
<b>Security Risk Management</b> Information security controls, threat detection, and incident response	Undefined	Noncommittal	Framework-Based	Framework-Based
<b>Terms of Use</b> Legal agreements, service terms, and contractual protections	Pro-Platform	Consumer-Grade	Business-Class	Business-Class+

**Table 2: Classification of GAI Tools by Safeguards**

We recommend lawyers focus on technical fundamentals over broad labels. Don't make security assumptions based on whether a GAI tool is licensed as a free or paid version or is marketed as a consumer or business version. For example, you might find a GAI tool that allows model training by default (making it more aligned with the consumer-level safeguards in Table 2) but also allows users to opt-out of model training (changing it to be more aligned with the business-level safeguards in Table 2). It is the actual safeguards, and not the marketing label, that matter most when protecting client information.

**(1) Authentication**

Authentication refers to the security measures that protect the login process for a third-party managed GAI tool. As illustrated in Table 2, a public GAI tool typically provides no controls (for example, the public version of ChatGPT can be used by anyone with an internet connection and does not require creating an account or logging in). Consumer-aligned tools typically allow users to create individual accounts but may lack advanced protections such as multi-factor authentication. Business-aligned tools should require multi-factor authentication, while enterprise-aligned tools usually offer more sophisticated account-management capabilities, such as single sign-on (SSO).

## (2) Model Training

As a general rule, lawyers should not transmit Confidential Information or Sensitive Personal Information to a GAI tool that permits the information to be used for model training. Security researchers have demonstrated serious data security risks when classified information is used to train models.<sup>29</sup> For example, in one widely discussed study, researchers demonstrated the ability to retrieve verbatim copies of personally identifiable information from an early OpenAI model even when the information was included in only one document in the training data.<sup>30</sup>

The indicators in Table 2 show that public GAI tools require users to consent to model training, while tools aligned with the consumer category typically allow users to opt-out of model training. GAI tools that are more closely aligned with the business and enterprise categories will have model training turned off by default and include contractual assurances that customer data will not be used for this purpose. In the Technical Addendum included with this Guide, we provide more details for how model training works and discuss potential narrow exceptions to the general rule against allowing Confidential Information to be used to train models.

## (3) Data Retention

Lawyers should investigate how long the GAI tool retains information, both after the lawyer deletes it from the user interface and after the service itself is terminated. The ideal data retention setting for GAI tools is “Zero Data Retention,” meaning that a lawyer’s information is never retained by the underlying transformer model, and it is permanently removed from the provider’s servers immediately after the lawyer deletes the data from the user interface.<sup>31</sup> Some GAI tools, despite being licensed as business-class tools and being subject to business-class privacy and security assurances, do not support Zero Data Retention, and therefore may be inappropriate for processing Sensitive Personal Information (especially without informed client consent).<sup>32</sup> Table 2 shows the retention policies for public and consumer aligned GAI tools are typically defined by the third-party provider, and users have limited or no control over how long their data is stored or when it is deleted. By contrast, business and enterprise aligned tools provide these controls directly to the users or organizational administrators.

Lawyers who use GAI tools to process Confidential Information or Sensitive Personal Information should understand that these tools retain data in multiple layers, and each layer might have its own retention

---

<sup>29</sup> Nat’l Inst. of Standards & Tech., *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1) (July 2024), <https://doi.org/10.6028/NIST.AI.600-1>.

<sup>30</sup> Nicholas Carlini et al., *Extracting Training Data from Large Language Models*, in *Proceedings of the 30th USENIX Security Symposium* 2633 (USENIX Ass’n 2021), <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>.

<sup>31</sup> See *Vertex AI and Zero Data Retention*, Google Cloud, <https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance> (last visited Sept. 14, 2025) (providing a detailed discussion of Zero Data Retention applied to GAI tools).

<sup>32</sup> See *How We’re Responding to The New York Times’ Data Demands in Order to Protect User Privacy*, OpenAI (June 5, 2025), <https://openai.com/index/response-to-nyt-data-demands> (last visited Sept. 14, 2025) (describing OpenAI’s various data retention capabilities for public, consumer, and business-class versions in response to the Preservation Order entered in *In re OpenAI, Inc., Copyright Infringement Litigation*, No. 25-md-3143 (S.D.N.Y. 2025)) (referencing *In re Openai, Inc.*, 2025 U.S. Dist. LEXIS 97943 (S.D.N.Y. Mar. 13, 2025)).

settings. We've included a more detailed discussion of layered GAI data retention in the Technical Addendum included with this Guide.

#### (4) Data Isolation

The level of data isolation in a GAI tool determines how closely your data is stored with that of unrelated third parties. Vendors who misconfigure their data isolation settings might expose sensitive information and allow unauthorized access to customer-specific data or resources.<sup>33</sup> As the sensitivity of the information being processed by a GAI tool increases, so too should the level of data isolation. Lawyers who use GAI tools to process Confidential Information or Sensitive Personal Information should document the isolation settings for those tools. To help with this, we've included a more detailed discussion of how data isolation works in the Technical Addendum included with this Guide. As shown in Table 2, a GAI tool that is aligned with the public and consumer categories typically provides only basic, and therefore higher-risk, forms of customer isolation. Business and enterprise aligned tools are built with stronger isolation, such as independently audited logical separation or customer-dedicated environments.

#### (5) Supply Chain Risk

GAI tools often rely on a network of downstream service providers that may process, store, or transmit the data you send to the system. Each subprocessor should apply administrative and technical safeguards appropriate to the sensitivity of the data. Lawyers should identify all subprocessors involved in providing and maintaining the GAI tool, evaluate whether their access to client data is necessary and proper, and confirm that each is bound by confidentiality and security obligations through contractual flow-down provisions. Table 2 describes public and consumer-aligned GAI tools as having few, if any, supply chain safeguards or published details about their supplier ecosystem. Business-aligned tools tend to provide full transparency for the privacy and security practices of its downstream vendors. Enterprise-aligned tools may also provide regulation-level supply chain protection (such as HIPAA Business Associate Agreements that address specific regulatory requirements for downstream providers).

#### (6) AI Risk Management Frameworks

Reputable GAI tool providers should publish or directly provide written assurances that they design, maintain, and test their models in accordance with recognized risk management frameworks.<sup>34</sup> These frameworks address areas such as data governance, security controls, bias mitigation, transparency, and incident response. By aligning with these standards, providers demonstrate that their systems have been evaluated against widely accepted criteria for safety, reliability, and trustworthiness. Lawyers should request documentation of the provider's risk management practices and confirm that those practices remain aligned with these evolving frameworks. This is an area in which industry standards and official frameworks are not yet well established; accordingly, our Table 2 designations should be understood to illustrate that

---

<sup>33</sup> *Multitenancy and Azure OpenAI Service*, Microsoft Learn (May 13, 2025), <https://learn.microsoft.com/en-us/azure/architecture/guide/multitenant/service/openai> (last visited Oct. 7, 2025).

<sup>34</sup> Examples include the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) and the Open Worldwide Application Security Project (OWASP) GenAI Security Project.

business and enterprise level GAI tools have more formally documented AI risk management controls that reference independently and globally established baselines.

## (7) Security Risk Management

As discussed throughout this Guide, many components of a GAI tool are not unique to artificial intelligence, and are in fact traditional network storage, transmission, and processing functions. Like any other cloud-based system, a hosted GAI tool should demonstrate compliance with established data privacy and security standards.<sup>35</sup> Providers that follow these standards help ensure that the underlying infrastructure supporting AI functions meets accepted industry benchmarks for confidentiality, integrity, and availability of data. Unlike AI risk management, cloud security risk management is supported by numerous mature and well-established security frameworks. To be properly within the business or enterprise categories of Table 2, a GAI tool provider should publish formal, written, and independently verified audits demonstrating compliance with the security frameworks referenced in this Guide.<sup>36</sup>

## (8) Terms of Use

When selecting a GAI tool, lawyers should obtain written contractual assurances covering the provider's privacy and security obligations. These assurances should address both the underlying transformer model provider and the application itself. Written commitments are necessary to ensure that the handling of client data complies with professional duties of confidentiality, applicable privacy laws, and agreed security practices. You may notice in Table 2 that we designated the enterprise level to provide "Business-Class+" Terms of Use. The *plus* symbol is meant to convey that enterprise licenses typically provide customer-specific negotiating flexibility and additional safeguards for regulated data (such as a HIPAA Business Associate Agreement or GDPR-compliant Standard Contractual Clauses). We've also included a GAI Terms of Use Checklist at Appendix 2 for lawyers to consider when licensing third-party managed tools.

In addition to these key safeguards, lawyers might also consider where their GAI tools physically store and process data (including conversations, documents, and other elements of GAI storage as discussed in more detail in the Technical Addendum). The physical location of these operations can significantly affect the protections afforded to that data, and the circumstances under which the data can be accessed or deleted. Processing location could also impact the contractual or regulatory obligations lawyers may have with respect to data provided by clients.

### (b) Self-Managed GAI Safeguards

Lawyers who choose to deploy a self-managed GAI tool assume responsibility, not only for client confidentiality, but also for the full range of security, availability, and compliance risks associated with hosting and operating the transformer model and its ancillary support structure. To assist in that process, we recommend consulting the Cybersecurity Information Sheet ("CIS") titled *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems*, authored by the U.S. National Security Agency's

---

<sup>35</sup> These may include, for example, SOC 2, CSA STAR, ISO 27001, GDPR, CCPA, and other globally recognized privacy and security frameworks.

<sup>36</sup> *Id.*

Artificial Intelligence Security Center, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the New Zealand National Cyber Security Centre, and the United Kingdom's National Cyber Security Centre.<sup>37</sup>

A comprehensive discussion on self-managed GAI tools is beyond the scope of this Guide. However, in addition to providing the CIS in Appendix 6, we summarize below several of the most important safeguards for those lawyers who are interested in deploying a self-managed GAI tool to consider:

- **Deployment Environment Security**: Self-managed tools must run in a hardened environment. Firms are responsible for applying secure configurations, enforcing strong access controls, segmenting networks, and adopting defense-in-depth practices across the entire deployment.
- **Supply Chain and Model Integrity**: Open-weight models and external data sources must be carefully validated. Law firms should confirm the digital integrity of key transformer components and maintain version control to protect against tampered or malicious models. For example, we are aware of incidents in which malicious models were downloaded from widely used distribution sites.<sup>38</sup>
- **Model Weight Protection**: The trained “weights” of a self-hosted model are highly sensitive. Lawyers must ensure that weights are stored securely, access is restricted to essential personnel, and exposure through APIs is minimized to reduce risks of exfiltration or inversion attacks.
- **Monitoring and Incident Response**: Self-managed deployments require continuous monitoring for anomalies and suspicious activity. Law firms or their outsourced IT providers should maintain logs, alerting systems, and a documented incident response plan that supports isolation, patching, and rollback of compromised systems.
- **Data Protection and Secure Deletion**: When no external provider manages storage, the firm is directly responsible for encryption, secure key management, and verified deletion of data, logs, and training inputs when no longer needed.
- **Patching and Updates**: Self-managed GAI tools require regular updates and security patches, both for the application itself and the underlying hardware or cloud environment. Before deployment, firms should also test whether their systems can be restored quickly and securely if something goes wrong.

Lawyers using self-managed systems may use the safeguards in the Cybersecurity Information Sheet (CIS, Appendix 6) to assess whether a system is appropriate for each information classification (Table 2) and to guide client communications (Table 3). The following non-binding examples show one way to document that approach:

---

<sup>37</sup> Nat'l Sec. Agency Artificial Intelligence Sec. Ctr. et al., *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems* (Apr. 2024).

<sup>38</sup> N.J. Cybersecurity & Commc'ns Integration Cell, *Hugging Face AI Platform's Problem with Malicious AI* (Mar. 7, 2024), <https://www.cyber.nj.gov/Home/Components/News/News/1216/214> (last visited Sept. 13, 2025).

- Enterprise-aligned. Professionally deployed; governed by written policies and procedures; periodic, framework-based security risk assessments that expressly address a self-managed GAI deployment (see CIS, Appendix 6).
- Business-aligned. Managed by individuals reasonably skilled in GAI deployment, system administration, and security configuration; uses business-class hardware, operating systems, and applications; employs prudent safeguards (e.g., strong authentication, encryption, regular updates); may lack a formal written security program or independent assessments.
- Consumer-aligned. Operated by individuals with limited security and administration experience; relies on default settings; lacks rigorous access controls or encryption; often uses personal-grade hardware/software not intended for client information.

These examples illustrate a method to evaluate and document how client information is processed and how client communications are managed in a self-managed environment.

In summary, while self-managed GAI tools avoid the risk of allowing a third-party to process and store client data, they also carry the heaviest operational burden. Firms that choose this path must be prepared to treat the GAI tool as part of their critical infrastructure, subject to the same rigor as their other on-premise servers and related network equipment. With the right planning, governance, and support, self-managed GAI tools can be a safe and effective option for processing highly sensitive client information, but they are not risk free.

## Managing Client Rights

By this point, you should have a basic understanding of how GAI tools work, and you should be capable of choosing appropriate GAI tools for all types of data we've discussed, including Confidential Information and Sensitive Personal Information. The next important idea is how best to communicate with clients when using GAI tools to process their matters, Confidential Information, and Sensitive Personal Information.

Taken as a whole, the approach presented in this Guide is a notice and opt-out paradigm, with enhanced protection for highly sensitive information. There are analogous examples within Illinois public policy. In the context of health information exchange systems, for example, the Illinois Health Information Exchange Authority determined that a notice and opt-out system would afford patients a greater degree of choice without the relatively burdensome documentation requirements of a more formal patient-by-patient consent system.<sup>39</sup> While not directly applicable to the use of GAI tools and the practice of law, the relationships described in this report (between technology, healthcare providers, and patients) parallel the relationships between artificial intelligence, lawyers, and their clients.

Client communication, including client notice, client opt-out rights, and informed client consent, should be understood as an additional safeguard that a lawyer might employ when using GAI tools, and not as a method of shifting risk from the lawyer to the client. In other words, lawyers must be reasonable when selecting and

---

<sup>39</sup> Ill. Health Info. Exch. Auth., Data Sec. & Privacy Comm., *Report of Preliminary Findings and Recommendations* (Sept. 19, 2012).

using GAI tools to process their data and simply obtaining a client’s consent cannot be used as a substitute for the due diligence we’ve outlined throughout this Guide.

The non-exclusive considerations identified in Comment [18] to Illinois Rule of Professional Conduct 1.6 remain relevant when evaluating the use of GAI tools:

1. The sensitivity of the information;
2. the likelihood of disclosure if additional safeguards are not employed;
3. the cost of employing additional safeguards;
4. the difficulty of implementing the safeguards; and
5. the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Although Comment [18] predates modern GAI tools, lawyers can still use its technology-neutral balancing test to determine what safeguards are appropriate when using GAI tools, including providing notice and opt-out rights, or, in appropriate cases, seeking informed client consent.

The table below shows one example of how a lawyer might use the GAI categories we reviewed in Step 3 above (public, consumer, business, and enterprise) to determine how best to manage client communications for different levels of information sensitivity. They are not endorsements and do not constitute legal advice.

Data Classification	Public	Consumer	Business	Enterprise
<b>General Information</b> Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
<b>De-Identified Information</b> No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
<b>Confidential Information</b> Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
<b>Sensitive Personal Information</b> Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
<b>System-Wide Processing</b> GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

**Table 3: Relationship between data classification, GAI tool classification, and client communication strategy**

In this example, the lawyer has determined that General Information (which we defined in Step 1 as information that is entirely unrelated to any matter the lawyer has undertaken professionally and is otherwise not subject to any confidentiality protections) does not require any client communication regardless of the level of safeguards incorporated into the GAI tool. Despite the fact that no client information is being processed, the lawyer should still exercise caution when entering information into a public GAI tool due to the absence of privacy and security safeguards.

With respect to De-Identified Information (which we defined in Step 1 as information that relates to the representation of a client, but for which there is no reasonable likelihood that it could be used to ascertain the identity of the client or matter), the lawyer has determined that clients should receive reasonable notice

and opt-out rights when this information will be processed by a consumer or business-class tool, but that an enterprise-grade tool has sufficient safeguards to allow unrestricted processing. By contrast, even if the lawyer determines it is reasonable to process De-Identified Information using a public tool, informed client consent is still advised prior to doing so.

With respect to Confidential Information (which we defined in Step 1 as information that is protected by Rule 1.6, or is otherwise subject to confidentiality obligations, but without Sensitive Personal Information), the lawyer has determined that it cannot be processed using a public GAI tool under any circumstances, but that business-class and enterprise-grade tools provide sufficient safeguards to allow processing with only notice and opt-out rights. In Step 2, we defined “public” to mean GAI tools that are operated and controlled by a third party and strongly aligned with the public category shown in Table 2. A lawyer might reasonably determine that Confidential Information can be processed using a consumer-aligned tool if the available security options described in Table 2 are enabled (such as, for example, opting out of model training) and informed client consent is obtained as an additional safeguard.

With respect to Sensitive Personal Information (which we defined in Step 1 to include highly sensitive elements such as medical records and financial accounts), the lawyer has determined that it cannot be processed using a public or consumer GAI tool under any circumstances. The lawyer has also determined that informed written consent should be obtained prior to processing this information using a business-class GAI tool that has not fully incorporated all the enterprise-level safeguards described in Table 2.

Clients and lawyers should also understand that certain types of GAI processing, described in Table 3 as “System-Wide Processing,” may be difficult or infeasible to disable. For example, if a major cloud platform (like Microsoft 365) begins actively incorporating GAI functionality into its basic computational structure, the law firm’s entire data repository could be subject to GAI processing, even involving Sensitive Personal Information. Clients should still be made aware that this processing happens, but there might not be a clear path for them to opt out. In these cases, and again using the five factors set forth in Rule 1.6, Committee Comment [18], a lawyer might conclude that even though the sensitivity of the information is high (factor 1), the difficulty of allowing opt-out rights for systemic AI processing (factor 4) and the extent to which allowing opt-out rights will adversely affect the lawyer’s ability to represent clients (factor 5) are too high. In such a case, the lawyer might choose to focus on reducing the likelihood of disclosure (factor 2) by allocating more resources to employing additional safeguards (factor 3). In that case, the lawyer should ensure that the tools used for system-wide processing are closely aligned with the enterprise-level safeguards shown in Table 2.

Rule 1.6 references informed consent in two different contexts, and the distinction is useful when managing GAI-related client conversations. Rule 1.6(a) states that lawyers may not “reveal information relating to the representation of a client unless the client gives informed consent.” This has not typically been interpreted to require informed consent when lawyers process client information through a third-party vendor, and it seems plausible that this understanding should continue in the context of third-party managed GAI tools.<sup>40</sup> However, Committee Comment [18] to Rule 1.6 also states: “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures

---

<sup>40</sup> See, e.g., Ill. State Bar Ass’n, Prof’l Conduct Advisory Op. No. 16-06 (2016). (“A lawyer’s use of an outside provider for cloud-based services is not, in and of itself, a violation of Rule 1.6, provided that the lawyer employs, supervises and oversees the outside provider.”).

that would otherwise be required by this Rule.” This latter use is particularly relevant to discussions about client notice, opt-out rights, and use of informed consent as an additional safeguard.

We align with the American Bar Association’s view that, where client consent is required, it must be informed.<sup>41</sup> This Guide focuses on implementation; lawyers retain professional judgment, consistent with Rules 1.4 and 1.6, to determine the nature and extent of client communication appropriate to the particular engagement and the type of data processing contemplated. To support that judgment, this Guide offers a Sample Notice of Artificial Intelligence Practices (Appendix 3) that firms may adapt for use in engagement materials or on firm websites. Firms may also designate a knowledgeable point of contact for AI-related client inquiries; depending on the firm’s structure, this may be a lawyer or a non-lawyer (e.g., a vendor or outsourced IT professional), subject to confidentiality and supervision obligations. Where more extensive AI processing or Sensitive Personal Information is involved, enhanced matter-specific explanations and informed written consent may be prudent.

### Key Takeaways

Summarizing everything we’ve discussed in this Section:

- The baseline for our hypotheticals and sample forms is that of a GAI tool aligned with the business category in Table 2. When using such a tool to process information that is classified no higher than Confidential Information (as defined in Step 1 of the Core Framework), lawyers are encouraged to provide clients with notice and a right to opt out. A sample notice form provided at Appendix 3.
- When processing Sensitive Personal Information, lawyers are encouraged to incorporate additional safeguards, such as those aligned with the enterprise category in Table 2 and/or seeking informed client consent. A sample informed consent form is provided in Appendix 5.
- Lawyers should exercise caution when using GAI tools that align with the public or consumer category in Table 2, even for De-Identified Information. Where a lawyer reasonably determines that such a tool is appropriate for limited use, it is generally prudent to also obtain informed client consent.
- As GAI becomes more integrated into our computers and applications, Lawyers and clients should understand that it may become infeasible to disable some GAI features. In such cases, lawyers are encouraged to focus on enterprise-aligned safeguards, where possible, to offset the infeasibility of providing clients with opt-out or consent rights.

We recognize that these concepts are evolving rapidly, and we do not expect lawyers to become artificial intelligence experts or dedicate extensive research to mastering every nuance in the universe of artificial

---

<sup>41</sup> ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 512 (July 29, 2024) (addressing Generative Artificial Intelligence tools) (“When consent is required, it must be informed. For the consent to be informed, the client must have the lawyer’s best judgment about why the GAI tool is being used, the extent of and specific information about the risk, including particulars about the kinds of client information that will be disclosed, the ways in which others might use the information against the client’s interests, and a clear explanation of the GAI tool’s benefits to the representation.”).

intelligence technology. Rather, the intent is to highlight reasonable considerations lawyers might apply in evaluating GAI tools consistent with their existing professional responsibilities. Lawyers should use informed judgement in selecting and monitoring GAI tools, provide clients with appropriate information when their data may be processed using such tools, and remain attentive to client questions or concerns about these emerging technologies.

## Implementing the Practice Resource Kit

To help lawyers document the various ideas presented throughout this Guide, we are providing a “Practice Resource Kit.” These materials are based on a hypothetical law firm named “ACME Law, LLC” and reflect a set of decisions and risk assessments that this hypothetical small firm has undertaken. Lawyers using these resources should do so very carefully to ensure the language finally used fits the particular situation for which they are designed. It is not the intent of these resources to suggest or establish practice standards. The following is a brief summary of each component of the Practice Resource Kit.

### GAI Terms of Use Checklist

The GAI Terms of Use Checklist, included as Appendix 2, is designed to help lawyers evaluate whether a provider’s contract terms adequately address the safeguards described in this Guide. It distills the key legal, ethical, and technical considerations into a practical review tool that can be applied when negotiating or reviewing agreements with GAI vendors. The checklist is not mandatory and does not constitute legal advice; lawyers are encouraged to adapt it to their own practice needs and the sensitivity of the data they intend to process.

### Sample Notice of Artificial Intelligence Practices

The Sample Notice of Artificial Intelligence Practices is attached as Appendix 3. We encourage lawyers and law firms to document their own risk assessments and decision-making processes when applying the GAI safeguards and making determinations about how to manage client communications. For example, lawyers might consider using the sample methodology provided in Table 2 and Table 3 above to document their selection of GAI tools and their corresponding client communication strategy.

### Sample Use of GAI Tools Policy

The Sample Use of GAI Tools Policy is intended to provide an example of the type of written policy that lawyers and law firms might use to ensure everyone in the firm is aligned about their responsibilities when using artificial intelligence. The Policy is designed to be distributed to everyone in the firm, including lawyers, staff, paralegals, and other individuals who have access to the firm’s resources.

The Sample Use of GAI Tools Policy assumes that a lawyer or law firm has already worked through the analysis outlined in the Core Framework section of this Guide and has selected appropriate GAI tools that will be made available to the workforce. Those tools are called “Approved GAI Tools” and should be listed on a Schedule of Approved GAI Tools as described in the Policy. The Sample Use of GAI Tools Policy also provides guidance for managing client rights and communications. Finally, the Policy is meant to address several other

ethical obligations that lawyers should observe when using GAI tools, such as retaining professional responsibility for GAI tool output, avoiding hallucinations, and candor towards the tribunal.

### Sample Informed Client Consent Form

As discussed throughout this Guide, there may be times when lawyers and law firms determine it is necessary or prudent to obtain informed client consent prior to using a GAI tool to process the client's information or matters. To assist with that process, we provide a Sample Informed Client Consent Form that lawyers and law firms might adopt for their own use.

In reviewing this sample form, we suggest lawyers reference the definition of informed consent provided in Rule 1.0(e). We also recommend considering the Federal Trade Commission's approach to "Affirmative Express Consent", which focuses on providing clear notice of the types of information to be processed and the purpose for which it's being used.<sup>42</sup>

Note also, as outlined in Section 6(d) of the Sample Use of GAI Tools policy, clients must have the authority to provide consent to all the personal information a lawyer intends to process using its GAI tools. Thus, if the data includes Sensitive Personal Information of separate third parties, it may be prudent to inquire whether the client possesses this authority.

### The Road Ahead

Artificial intelligence changed almost daily as this Guide was written. Rather than attempting to track every change, we have focused on core principles that are likely to remain constant as GAI becomes more deeply embedded in the practice of law. Our aim is to help lawyers adapt thoughtfully, regardless of which new tools, models, or regulations emerge in the months and years ahead.

For example, we believe the fundamental concept of the transformer model as expressed in the *Attention Is All You Need* research paper is likely to persist as a bedrock algorithm throughout the foreseeable development of GAI-powered legal applications. We also believe transformer models will continue to be utilized via the basic pathways we've described in the Core Framework section (Native Model Platforms, API integrations, and self-managed downloadable GAI models).

Still, we see new implementations of these basic concepts emerging quickly. For example, as this Guide is being written, "agentic" AI systems are starting to become mainstream. Agentic systems have the ability to access information on their own and take action directly. For example, we're not far from a future in which lawyers can instruct their AI agents to book a trip out of town and reliably expect the agent to review the available flight and hotel accommodations, choose the best room and flight, and then book the trip directly.<sup>43</sup> Clearly, this level of access and autonomy will raise a variety of novel risks; accordingly, we intend to track these developments closely and update the Guide regularly.

---

<sup>42</sup> *In re X-Mode Social, Inc. & Outlogic, LLC*, Docket No. C-4802 (F.T.C. 2023).

<sup>43</sup> Anjanava Biswas & Wrick Talukdar, *Building Agentic AI Systems* (Packt Publishing 2025).

Our working view is that, when used with appropriate safeguards, artificial intelligence can strengthen legal practice, including for solo and small firms. Lawyers should continue to exercise diligence, care, and adaptability. Prudent practices include remaining curious, applying appropriate safeguards, documenting decisions, and maintaining meaningful human oversight.

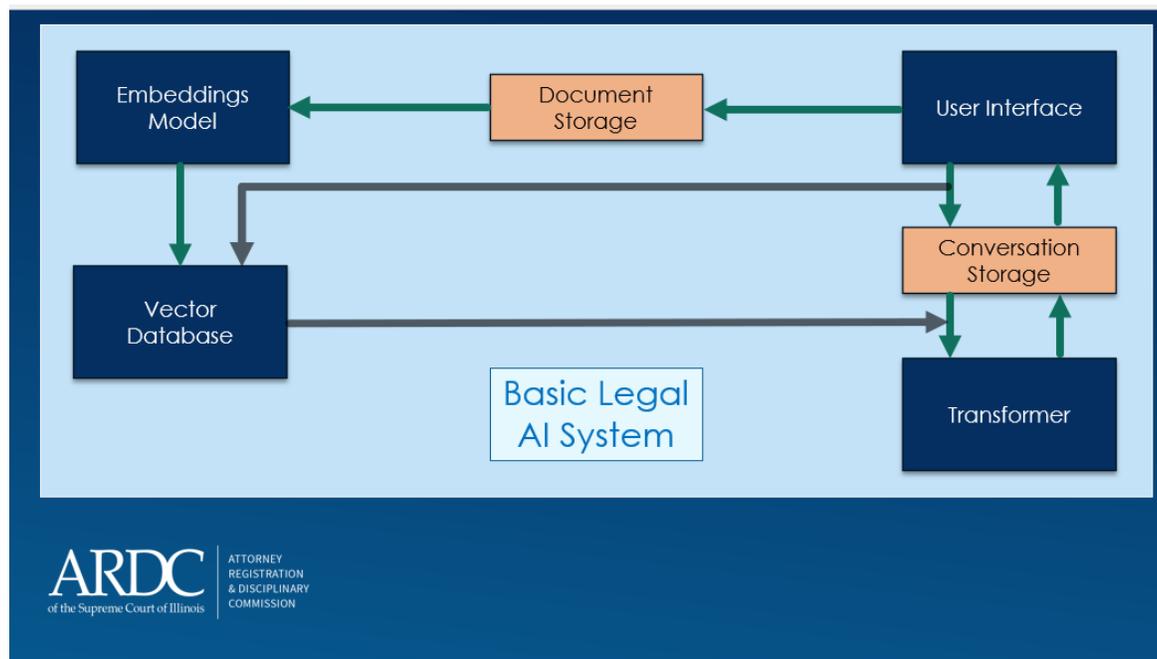
We look forward to taking this journey together and supporting you along the way.

## Technical Addendum

In the main body of this Guide, we presented the Core Framework for evaluating GAI tools for use with different levels of data sensitivity. That framework is sufficient to responsibly choose and implement GAI tools in most legal practices. However, some lawyers may wish to explore these issues in more detail (particularly when considering tools that will store or process highly sensitive or regulated data).

This Technical Addendum illustrates how typical GAI systems work and provides a deeper analysis of key GAI safeguards that comprise the Core Framework. The concepts outlined here apply broadly to most GAI tools, including ChatGPT, Claude, Gemini, Copilot, and many AI-driven legal industry tools. At a high level, these systems share the same essential building blocks; thus, understanding this model can help lawyers more easily evaluate and compare the tools they are likely to encounter in practice.

Figure 2 illustrates the major components of a typical GAI system:



**Figure 2: Functional Diagram of a Basic Legal AI System.** This model shows how user prompts interact with stored documents and conversation history, using embeddings, retrieval augmented generation, and a transformer-based language model to generate responses.

Most of the lawyer’s experience takes place in the user interface, which is where we log into the application, manage settings, engage in AI conversations, and upload documents for use within the GAI tool. Behind the scenes, however, there’s a lot going on.

### Model Training

The Core Framework introduced the transformer model and explained why it is the essence of any GAI tool. We also cautioned lawyers about the risks associated with model training and identified the ability to disable model training as a principal safeguard for protecting client information.

Training is the method by which a model provider sets the "weights" or "parameters" of the transformer models they produce. Think of a model weight like a pre-set multiplier that is used to process any kind of input that a human user might provide. Figure 3 provides a visual representation to help conceptualize this idea.

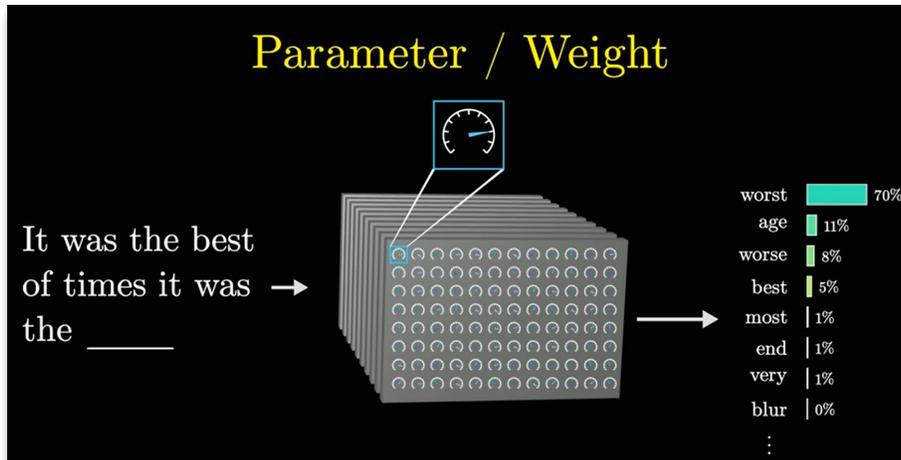


Figure 3: Conceptualization of transformer model weights being set during training. Image courtesy of 3Blue1Brown.com.

LLMs work by multiplying the numeric values of input text against a set of "weights" or "parameters" that are set while a model is being built.<sup>44</sup> This weighted multiplication operation happens each and every time a new word<sup>45</sup> is processed by the model, resulting in the entire vocabulary of the model being ranked from most to least likely as the next appropriate word.<sup>46</sup> In the specific example depicted in Figure 3, the model has ranked the word "worst" as the most likely next word, because its numeric weights produced that outcome when multiplied through.

Before a model is trained, its internal numeric weights are initialized with no patterns at all, effectively just random numbers.<sup>47</sup> Thus, if you ask an untrained model to finish the sentence "It was the best of times it was the \_\_\_\_\_", the untrained model is likely to respond with randomly selected words from its default vocabulary such as "It was the best of times it was the lorem ipsum."

In simple terms, a large language model (LLM) is trained by providing it with a large body of pre-existing text, one word at a time, and directing it to guess each successive word before it is revealed. If the model guesses correctly, that outcome is reinforced. If it guesses incorrectly, its internal weights are adjusted to

<sup>44</sup> Jay Alammar & Maarten Grootendorst, *Hands-On Large Language Models* (O'Reilly Media 2024).

<sup>45</sup> Technically, the term is "tokens," but we have opted to reduce the use of technical terms in this Guide to promote readability.

<sup>46</sup> Alammar & Grootendorst, *supra* note 44.

<sup>47</sup> Andrew Glassner, *Deep Learning: A Visual Approach* (No Starch Press, June 2021) (explaining that neural network training begins with random weights, producing meaningless output until adjusted through learning).

reduce the error.<sup>48</sup> As this process continues across millions and millions of words, the weights become increasingly precise, and the model's output begins to sound more like the data it was trained on.<sup>49</sup>

## Conversation and Document Storage

GAI tools are typically built around traditional storage systems that are not significantly different from any other cloud-based service. In most GAI tools, these databases hold conversation history, documents, and other interactions with the system. We've illustrated these components in Figure 2 above using orange shading. Following the flow shown in Figure 2, the user might enter text or a document into the user interface (such as, for example, asking ChatGPT a question). That text or document is then formatted into an AI-compatible form and sent to the transformer model to be processed. The transformer returns a human-readable response. The combination of the user's input (or "*prompt*") and the transformer's output now forms a conversation which is stored in the same type of cloud storage that any other text-based information might be stored.

Retention settings for these databases determine how long content remains accessible after a user deletes it, and how long it is retained after an account is closed. Deleted items may also remain in backup storage for weeks or months before being permanently removed, depending on the provider's policies.<sup>50</sup>

Based on our review of several major model providers, deleted conversations are generally removed from the provider's systems within a fixed period (often about 30 days). Enterprise-grade systems may offer additional protection, such as:

- Administrative controls that allow the organization to set retention limits for conversations, removing this discretion from individual users;
- Account configurations that give the customer direct, unilateral control over storage areas holding documents, conversation history, and other model outputs; and
- Encryption of traditional storage containers at rest within the provider's platform.

Because the traditional database layer often contains the most complete record of a user's interactions with the GAI tool, it is critical for lawyers to determine whether these retention periods and controls are appropriate for the sensitivity of the data being stored.

There are a few reasons we feel that lawyers should understand the distinction between AI components and traditional storage and networking components. First, having this understanding can help demystify the overall idea of using GAI tools. It's helpful to think of these systems as traditional computer and cloud services that have the addition of transformer-based processors. Second, the AI components used to process and store

---

<sup>48</sup> Matthew Burtell & Helen Toner, *The Surprising Power of Next-Word Prediction: Large Language Models Explained, Part 1*, Ctr. for Sec. & Emerging Tech., Georgetown Univ. (Mar. 8, 2024), <https://cset.georgetown.edu/article/the-surprising-power-of-next-word-prediction-large-language-models-explained-part-1> (last visited June 18, 2025).

<sup>49</sup> See, e.g., *ChatGPT Consumer Terms of Use*, OpenAI (Dec. 11, 2024), <https://openai.com/policies/terms-of-use> (providing that, unless users opt out, OpenAI may use content submitted through ChatGPT to improve its models).

<sup>50</sup> *AI Logs and Legal Holds: How to Build a Defensible Retention Strategy*, Hanzo (Sept. 17, 2025), <https://www.jdsupra.com/legalnews/ai-logs-and-legal-holds-how-to-build-a-7261821> (last visited October 1, 2025).

data present different types of privacy and security risks than traditional components. In general, understanding which parts of the system are AI-based and which parts are not can help lawyers make better decisions about client confidentiality, vendor due diligence, and ethical compliance.

## Retrieval-Augmented Generation

Many GAI tools use retrieval-augmented generation (“RAG”) to help reduce hallucinations and provide the system with specific knowledge about individual situations. The RAG database might be provided by an entirely separate company, and these databases often store verbatim confidential information for extended periods. Because RAG databases can retain sensitive data and operate largely behind the scenes, it is important for lawyers to verify what subcontractors are involved in managing the GAI tool, including the RAG database and what privacy and security assurances apply across the entire supply chain.

The RAG process is depicted using grey arrows in Figure 2 and can be understood as follows:

- *First*, the user enters a prompt into the user interface (such as, for example, asking ChatGPT a question). Normally, this would be sent directly to the transformer model for processing, but, since the system uses RAG, something else happens behind the scenes.
- *Second*, the user’s prompt is redirected to a special type of AI-compatible database. The purpose of this database is to hold specific information the user is likely to need in a way that is pre-formatted for processing by the transformer model. For example, in a legal research system, the AI-compatible database might hold statutes, cases, law review articles, and other law-related resources.
- *Third*, the system pulls relevant snippets of AI-formatted information from the AI-compatible database and prepends this additional information to the user’s original prompt.
- *Fourth*, the combination of the user’s original prompt and the augmented information from the AI-compatible database is sent to the transformer model for processing.
- *Finally*, the transformer model generates output in response to the user’s augmented input. In other words, the transformer model’s generation is *augmented* by what it has *retrieved* from the AI-compatible database, so we call it “*retrieval-augmented generation*.”

While lawyers do not need to understand the technical details of how RAG and AI-compatible databases function, lawyers *should* understand that multiple providers are likely to be involved in the process of storing, processing, and transmitting information that moves through a typical GAI system. One provider might supply the transformer model, while a different provider might supply the RAG database. When reviewing any cloud-based system used to store, process, and transmit confidential information, it’s important to have a basic understanding of what third parties have access to that information and what privacy and security assurances are in place to support these disclosures.

## Data Retention Within the Model

As we’ve learned, the portion of a GAI tool that performs the actual “artificial intelligence” processing is the transformer model. Accordingly, a key data retention issue to consider is whether the transformer model

itself retains any data that it processes and, if so, for how long. Based upon our review of several major model providers, we believe data retention at the transformer level falls broadly into the following categories:

- By default, model providers tend to keep data for a fixed period (typically 30 days) after it is processed.
- With specific approval, model providers may agree to convert the transformer to Zero Data Retention. With this configuration in place, the model will not retain any data that it processes.

Lawyers using a Native Model Platform must negotiate and manage the transformer’s retention period directly. By contrast, if a lawyer’s application is based on an API Integration, it is the application provider, and not the lawyer, who controls this setting. A transformer operating in Zero Data Retention mode is generally more appropriate for processing sensitive information, including Sensitive Personal Information.

### Data Retention for Abuse Monitoring

Closely related to transformer-level retention, many GAI tools also log user inputs and outputs for abuse monitoring purposes. These logs are intended to detect and prevent prohibited activities such as malicious code generation, harassment, or other uses that violate the provider’s terms of service.<sup>51</sup>

By default, model providers are likely to retain abuse monitoring logs for a defined period, often 30 days, even if the transformer’s data retention is set to Zero Data Retention. These logs may contain user content, and they may be reviewed by human moderators or analyzed automatically for compliance purposes.<sup>52</sup> Some providers allow these logs to be disabled or to operate in a Zero Data Retention mode for approved accounts. Due to the risk of storage and disclosure, systems with abuse monitoring logs disabled are generally more appropriate for processing sensitive information.

### Data Isolation

Anytime you store or process data in a cloud environment, there is some level of resource sharing among the customers of that service. In a fully multi-tenant environment, most of the components of the environment are shared by all customers of the service, subject only to basic logical separation. Multi-tenant environments are less expensive, but they increase the risk of data leakage between customers. Isolated environments tend to be more expensive but are also more appropriate for storing and processing highly sensitive data.

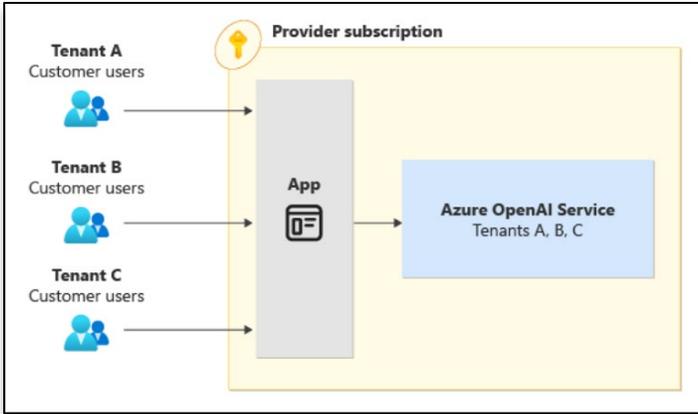
Figure 4 below shows how a GAI tool developer might deploy their architecture within the Microsoft Azure OpenAI service.<sup>53</sup> As stated by Microsoft “this solution is the easiest to implement, but it provides the least data isolation and performance isolation.”

---

<sup>51</sup> *Abuse Monitoring*, Microsoft Learn (Sept. 30, 2025), <https://learn.microsoft.com/en-us/azure/ai-foundation/openai/concepts/abuse-monitoring> (last visited October 2, 2025).

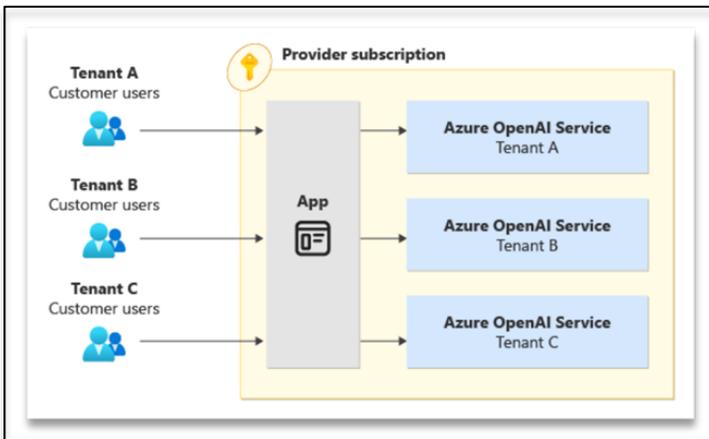
<sup>52</sup> *Id.*

<sup>53</sup> *Multitenancy and Azure OpenAI Service*, *supra* note 33.



**Figure 4: Illustration of an AI system deployment using the Microsoft Azure OpenAI isolated tenant configuration.**

By contrast, Figure 5 below shows another option that GAI tool developers might choose to better isolate their customers’ data. As described by Microsoft “this approach provides data isolation for each tenant [but] it requires you to deploy and manage an increasing number of Azure OpenAI resources as you increase the number of tenants.”



**Figure 5: Illustration of AI system deployment using Microsoft Azure OpenAI multi-tenant configuration.**

The more sensitive the data, the more carefully a lawyer should examine the provider’s data isolation practices and require that the agreement include explicit safeguards addressing data isolation.

## Supporting Resources and Materials

---

Appendix 1: Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI

Appendix 2: GAI Terms of Use Checklist

Appendix 3: Sample Notice of Artificial Intelligence Practices

Appendix 4: Sample Use of GAI Tools Policy

Appendix 5: Sample Informed Client Consent Form

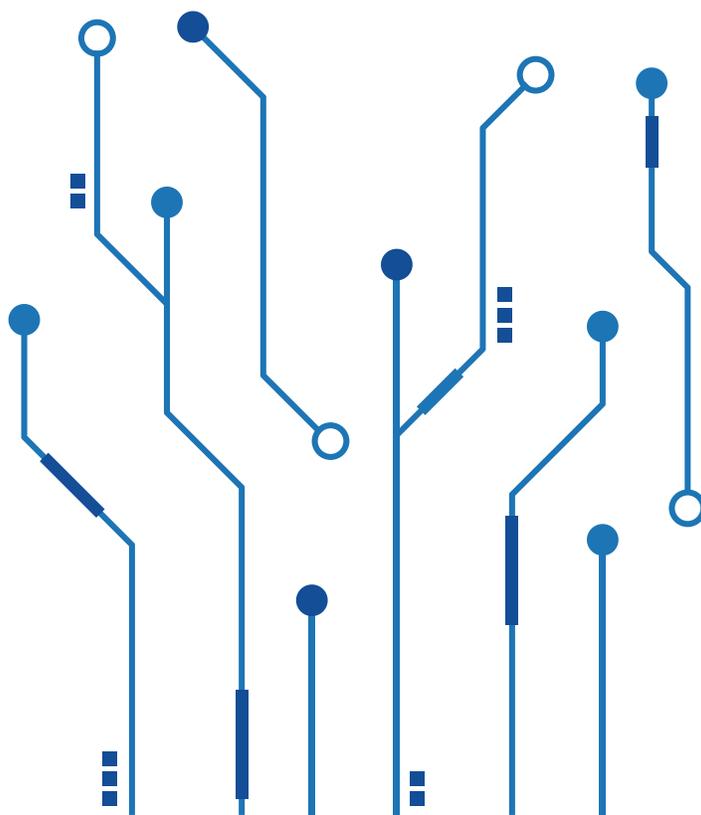
Appendix 6: Cybersecurity Information Sheet (“CIS”): Deploying AI Systems Securely – Best Practices for Deployment

**Appendix 1**  
**Illinois Supreme Court Policy on Artificial Intelligence,  
together with Judicial Reference Sheet on AI**



# ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

EFFECTIVE JANUARY 1, 2025



Embracing the advancements of artificial intelligence (AI), the Illinois Supreme Court remains steadfast in its commitment to upholding the highest ethical standards in the administration of justice. We acknowledge the rapid development of generative AI technologies capable of producing human-like text, images, video, audio, and other content. The integration of AI with the courts is increasingly pervasive, offering potential efficiencies and improved access to justice. However, it also raises critical concerns about authenticity, accuracy, bias, and the integrity of court filings, proceedings, evidence, and decisions. Understanding the capabilities and limitations of AI technology is essential for the Illinois Judicial Branch.

The Illinois Courts will be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice. Unsubstantiated or deliberately misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making will not be tolerated.

The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.

The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations. Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

This policy reflects the Illinois Supreme Court's commitment to upholding foundational principles while exploring the potential benefits of new AI technologies in a dynamic landscape. The Court will regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice. **Judges remain ultimately responsible for their decisions, irrespective of technological advancements.**

The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice. To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI.





# ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE JUDICIAL REFERENCE SHEET

JANUARY 1, 2025

## WHAT IS ARTIFICIAL INTELLIGENCE?

Technology that simulates human intelligence, enabling machines to learn, reason, perceive, and make decisions.

**Artificial Intelligence is not new technology.**

### 1950s Origins of AI

**Examples:** Spell check, predicative typing, facial recognition, and computer based legal research.

### 2022 Mainstream Availability of Generative AI

**Examples:**

#### Text Composition Prompts

“Summarize the following legal brief and identify key arguments.”

“Rewrite this paragraph in a respectful and neutral tone using plain language so it can be understood by people without legal expertise.”

“Prepare a speech about the importance of procedural due process for an audience of judges.”

#### Photo/Audio/Video Prompts

“Create image of an Illinois Courtroom.”

“Create movie depicting President Abraham Lincoln conducting legal research on a computer.”



## WHAT IS GENERATIVE ARTIFICIAL INTELLIGENCE?

A subset of artificial intelligence focused on creating new content, such as text, images, and video, by learning from existing data.

**Generative AI is a relatively new tool.**

## WANT TO KNOW MORE?



[National Center for State Courts AI Resource Center](#)



[Description of AI and Court Use Cases Video](#)

## JUDICIAL DECISIONS

Judges remain ultimately responsible for their decisions, irrespective of technological advancements.



### Code of Judicial Conduct - Rule 2.7

A judge shall hear and **decide** matters assigned to the judge...



### Code of Judicial Conduct - Rule 1.2

A judge shall act at all times in a manner that promotes public confidence in the independence, integrity, and impartiality of the judiciary...

## PLEADINGS

Lawyers & Self Represented Litigants are subject to sanctions for submitting legally or factually unfounded pleadings.



### Illinois Supreme Court Rule 137

The signature of an attorney or party constitutes a certificate by him that he has read the pleading, motion or other document; that to the best of his knowledge, information, and belief formed after reasonable inquiry it is well grounded in fact and is warranted by existing law...

# THINKING ABOUT USING GENERATIVE AI? JUDICIAL AI UTILIZATION GUIDELINES



**Ethical Oversight** - The Code of Judicial Conduct applies fully to the use of AI technologies. You maintain ultimate responsibility for all rulings and legal documents.



**Attribution** - Ensure your work product does not infringe upon copyright or intellectual property rights by proper attribution to sources as necessary.



**Competence** - The judicial branch must stay informed about evolving AI technologies. Prior to using any technology, including generative AI applications, you need to understand both general AI capabilities and the specific tools being used.



**Confidentiality** - If using a public generative AI tool (like ChatGPT), your input prompt is being handed over to the technology. Ensure you do not compromise sensitive information. Do not input any information such as (non-exhaustive list):

- Confidential or privileged information;
- Personal identifying information;
- Protected health information;
- Justice and public safety information;
- Code containing passwords or security-related information; and
- Information that has potential to erode public trust.



**Accuracy** - Be mindful that content from generative AI applications comes from sourced material. AI-generated content must be thoroughly reviewed to ensure accuracy and compliance with legal and ethical obligations, including a specific need to guard against technology lending to unintentional bias or prejudice.

## WHAT TO WATCH FOR AS A JUDGE

AI is ubiquitously present in modern technology. It is safe to assume AI was used in pleadings and other written materials. Generative AI applications gives rise to these considerations:



**Hallucinations** - When generative AI produces output that appears realistic but is misleading or made up by the AI itself rather than real-world data or input. If generative AI was used in a legal pleading or brief, included citations may be entirely made up or be a real case but not contain the purported language cited. [Read a case decision on hallucinations.](#)

### CHECK CITATIONS



**Deepfakes** - When generative AI is intentionally used to produce convincing/deceptive media - images, audio, video, etc. Fake evidence is relatively easy to create and reliable technology solutions do not exist to identify real vs fake evidence. [Learn more about identification of deepfakes.](#)

### HEAR EVIDENCE ON FOUNDATIONS



**Extended Reality** - Technology can seamlessly be integrated with our person through wearable devices. Recognize that technology may allow an individual to record and analyze audio and video and channel information from other sources in real-time, potentially without detection. [Learn more about extended reality.](#)

### ENFORCE EXISTING TECHNOLOGY RULES



## Appendix 2

### GAI Terms of Use Checklist

To assist with choosing appropriate third-party managed GAI tools, we prepared the following checklist. This is intended to help identify and evaluate important contractual protections, but should not be interpreted as a mandatory or exhaustive set of requirements.

- No Model Training: Neither the model provider nor any integrated application provider may use customer data to develop or improve its services without explicit, written customer consent.
- Purpose Limitation: Use of customer data should be limited to providing the services, complying with applicable law, enforcing provider policies, and preventing abuse. These purposes may be further limited where Zero Data Retention is enabled.
- Data Retention: Customer data must be permanently deleted from the provider's servers within a reasonable period after it is deleted from the user interface, or after account termination, except where retention is required by law.
- Data Isolation: Where higher degrees of data isolation are critical for the type of data being processed, the contract should address the specific isolation requirements for both the application and the transformer model.
- Data Residency: Where specific geographic hosting location is critical for the type of data being processed, the contract should specify the permitted data processing jurisdictions and include any applicable supplemental provisions (e.g. a Data Processing Addendum).
- User Anonymity: Where anonymous GAI inputs are critical to user privacy, the provider must ensure API requests do not include identifiable client or firm information.
- Compliance with Privacy Laws: Provider must comply with all privacy laws applicable to the data, customer, and clients.
- Breach Notification: Providers should clearly agree to provide timely breach notification requirements and specify their incident response obligations.
- Risk Management: The application must be developed, deployed, and maintained in accordance with recognized information security frameworks (such as SOC 2, ISO 27001, CSA STAR) and AI risk management frameworks (e.g., NIST AI RMF, OWASP GenAI Security Project). The provider should publish or provide supporting documentation demonstrating compliance.
- Third-Party Access Controls: Define and limit third-party access rights and include an obligation of the primary provider to bind downstream third parties to all relevant data management obligations.
- Supplementary Agreements: Explore the availability of a Data Processing Addendum for personal data processing or a HIPAA business associate agreement when required for protected health information.

The specific protections to include will depend on the type of data being processed, applicable regulations, and the lawyer's professional obligations in the given context.

## Appendix 3

### Sample Notice of Artificial Intelligence Practices

---

#### **SAMPLE NOTICE OF ARTIFICIAL INTELLIGENCE PRACTICES**

Acme Law, LLC provides this Notice of Artificial Intelligence Practices to explain how and when artificial intelligence tools may be used in providing our services. We believe it is important for clients to understand the circumstances under which personally identifiable information and client confidential information may be processed using artificial intelligence, the safeguards we apply to protect that information, and your rights relating to our use of such tools.

#### *GENERATIVE ARTIFICIAL INTELLIGENCE DEFINED*

When lawyers refer to “AI,” they are typically referencing a specific type of computer algorithm that predicts and generates text by analyzing patterns in numerical representations of language and images. These algorithms are often referred to as *Generative Artificial Intelligence* (“GAI”).

#### *HOW WE USE AI*

Some of our systems and professionals use business-class GAI tools. The attached Schedule of Generative Artificial Intelligence Tools provides representative examples of the tools we use.<sup>54</sup> Clients who have an active matter with us may request a current list of our GAI tools using the information provided at the end of this Notice. Our GAI Tools are used in the following contexts:

- System-Wide Processing. “System-Wide Processing” means using GAI systems in firm-wide administrative, security, or operational tools as part of standard functions, such as document management, email filtering, cybersecurity, or automated billing.
- De-Identified Processing. Some professionals at Acme Law, LLC may use GAI tools as work assistants without inputting any personally identifiable or client confidential information. When this type of processing relates directly to an active matter, clients have opt-out rights as described under “Your Rights” below.
- Confidential Processing. Professionals may, in some cases, use GAI tools to process personally identifiable or client confidential information. For example, a document may be uploaded to a GAI tool to support efficient review of that document. Clients have consent and opt-out rights for this type of processing, as described under “Your Rights” below.

---

<sup>54</sup> Lawyers may consider omitting the schedule of representative tools entirely, removing it from public-facing materials, or limiting distribution to active clients who request more information.

## *HOW WE PROTECT YOUR INFORMATION*

We maintain a formal written policy to ensure responsible and secure use of Generative Artificial Intelligence (GAI) tools. Among other things, our written policy provides the following safeguards:

- We take direct professional responsibility for the output of any GAI tool used in connection with our work. We believe GAI tools help make lawyers more efficient, but we do not rely on them to make legal judgments or decisions.
- When GAI tools are used for System-Wide Processing, we take reasonable and appropriate measures to ensure those tools are suitable for handling such protected information.
- We review all GAI tools for compliance with appropriate privacy assurances and security requirements before use. We do not use consumer-grade GAI tools such as the free or personal versions of ChatGPT.
- We maintain a written policy and train all lawyers and staff members to ensure that your rights, described below, are honored.

## *YOUR RIGHTS*

Clients have the right to remain informed about how GAI tools may be used in matters we undertake for them. We will regularly update the attached Schedule of Generative Artificial Intelligence Tools, and clients with an active matter may request a current version at any time.<sup>55</sup>

Clients may opt out of De-Identified Processing and Confidential Processing (defined above). To exercise this right, send us written notice using the contact information provided below.

Other than for System-Wide Processing, we will not use GAI tools to process information listed in the Illinois Personal Information Protection Act without your informed written consent. Individual clients may provide consent for use of their data directly. Organizational clients may provide consent if they are the lawful controller or processor of the data or are otherwise permitted to consent under applicable law. Consent may be revoked any time and for any reason. Revocation applies prospectively from the date it is received.

If we use GAI tools for System-Wide Processing (as defined above), we will take reasonable and appropriate measures to ensure such tools are suitable for processing personally identifiable and client confidential information.

### **Contact Information**

Johnathan A. Doe, Managing Partner  
ACME Law, LLC  
1234 Justice Lane, Suite 800  
Sampleville, IL 54321  
Phone: (555) 867-5309  
Email: [jdoe@acmelawfictional.com](mailto:jdoe@acmelawfictional.com)

**Effective Date:** October 1, 2025

---

<sup>55</sup> Refer to note 54.

## SCHEDULE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS<sup>56</sup>

The following table sets forth the Generative Artificial Intelligence tools in use at ACME Law, LLC as of the Effective Date of this Notice. Clients having an active matter with us may request a current list of our GAI tools using the contact information in this Notice.

Tool <sup>57</sup>	Representative Uses	Provider Safeguards
ChatGPT Team	document summarization or analysis, drafting assistance	<a href="https://trust.openai.com">https://trust.openai.com</a>
Microsoft Copilot	AI integrations in Microsoft Office and Teams	<a href="https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy">https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy</a>
Adobe AI Assistant	Document summarization and analysis	<a href="https://experienceleague.adobe.com/en/docs/experience-platform/ai-assistant/privacy">https://experienceleague.adobe.com/en/docs/experience-platform/ai-assistant/privacy</a>
vLex	Legal research, document drafting and analysis	<a href="https://trust.vlex.com">https://trust.vlex.com</a>
Lexis+AI	Legal research, document drafting and analysis	<a href="https://www.lexisnexis.com/pdf/rlex-responsible-ai-principles.pdf">https://www.lexisnexis.com/pdf/rlex-responsible-ai-principles.pdf</a>
CoCounsel	Legal research, document drafting and analysis	<a href="https://help.casetext.com/en/collectio ns/6255626-trust-security-and-privacy">https://help.casetext.com/en/collectio ns/6255626-trust-security-and-privacy</a>

The GAI tools listed above may rely on third-party providers and infrastructure to deliver their services. We enter into agreements with these providers that require appropriate privacy and security safeguards throughout the supply chain, including confidentiality, data protection, and access control measures.

---

<sup>56</sup> Refer to note 54.

<sup>57</sup> ARDC does not recommend or endorse any specific technology or provider. The examples given in this table are simply provided to illustrate how a typical law firm might choose to disclose the GAI tools it uses.

**Appendix 4**  
**Sample Use of GAI Tools Policy**

<b>POLICY</b> Use of GAI Tools	
<b>Policy ID:</b> AI G-100.1	<u>References:</u> <ul style="list-style-type: none"> <li>❖ <a href="https://openai.com">https://openai.com</a></li> <li>❖ <a href="https://www.microsoft.com/en-us/ai">https://www.microsoft.com/en-us/ai</a></li> <li>❖ <a href="#">Illinois Supreme Court Policy on Artificial Intelligence</a></li> <li>❖ <a href="#">Illinois Rule of Professional Conduct Rule 1.1 (Competence)</a></li> <li>❖ <a href="#">Illinois Rule of Professional Conduct Rule 1.4 (Communication)</a></li> <li>❖ <a href="#">Illinois Rule of Professional Conduct Rule 1.6 (Confidentiality of Information)</a></li> </ul>
Approved By:  <hr style="width: 20%; margin-left: 0;"/> Johnathan A. Doe, Managing Partner	

1. **Purpose.** This Policy addresses the use of Generative Artificial Intelligence (as defined below) at ACME Law, LLC. (“ACME”). Generative Artificial Intelligence is a rapidly evolving technology that can bring great value to our efforts. However, its legal and technical risks are not well-known, and its potential for unintentional misuse merits a consistent policy-based approach to using this technology within our environment.
  
2. **Scope.** This Policy applies to all members of the ACME Workforce. The term “ACME Workforce” means ACME employees, as well as independent contractors, interns, volunteers, and other individuals who are appointed or engaged to provide services or create work product on ACME’s behalf.

This Policy does not apply to activities outside the scope of one’s work for ACME unless such activities adversely affect the confidentiality, security, or reputation of ACME.

This Policy covers all company systems, devices, technologies, and platforms, including software applications, hardware devices, cloud platforms, mobile applications, and any other technology interfaces.

3. **Definition of Generative Artificial Intelligence.** For purposes of this Policy, the term “Generative Artificial Intelligence” or “GAI” refers to an artificial intelligence tool that is designed to produce new, previously unseen, data in response to human input using predictive algorithms applied to an underlying database of training data and may include systems that generate new images, text, sounds, or other data types in response to human input.

4. Approved GAI Tools. The ACME Managing Partner may designate one or more GAI tools as approved for use by the ACME Workforce (each an “Approved GAI Tool”). Approved GAI Tools will be posted at [*insert link or document ID*] (the “Schedule of Approved GAI Tools”). Only Approved GAI Tools may be used on ACME devices or to process ACME information (including ACME client information).
5. Professional Responsibility. Members of the ACME Workforce who use Approved GAI Tools may do so solely as supplementary instruments, such as to generate ideas or assist in the review or preparation of documents. While GAI can serve as a valuable tool, ultimate responsibility for the accuracy, relevance, and appropriateness of any final work product rests solely with the ACME Workforce member using the Approved GAI Tool.
  - (a) General Rule. GAI Tools are prone to generate fictitious case and statutory citations (a phenomenon often referred to as a “*hallucination*”). Accordingly, except as provided in Section 5(b), it is imperative that all outputs derived from Approved GAI Tools be meticulously reviewed, validated, and edited as necessary by the user before finalization. Use of Approved GAI Tools should not substitute or diminish the critical thinking, judgment, and expertise that our ACME Workforce members bring to their respective roles.
  - (b) Exception for Mass Data Processing. Where the value of using an Approved GAI Tool would be diminished by the requirement that all GAI outputs be meticulously reviewed and validated, the ACME Managing Partner may grant case-by-case exceptions to Section 5(a). For example, ACME might use an Approved GAI Tool to search or summarize large datasets that cannot reasonably be validated by humans or even traditional computer algorithms. In this example, requiring the output of the GAI process to be reviewed and validated by humans might defeat the purpose of using the GAI tool.
  - (c) Client Consent for Allocation of Responsibility. In such cases where ACME cannot reasonably exercise full professional responsibility for the GAI output, the client’s informed written consent shall be obtained as described in Section 6(c). The responsible attorney should consult Illinois Rule of Professional Conduct 1.2 when structuring a matter in this way.
6. Client Rights. Our clients have a right to be informed about how ACME uses GAI tools to process their matters and confidential information. This section outlines the rules for informing clients about our use of GAI tools. This section also describes when and how clients may opt out of our use of GAI tools to process their matters and confidential information. This section also describes the circumstances under which we are required to obtain a client’s informed written consent prior to processing their information using a GAI tool.
  - (a) Notice of Artificial Intelligence Practices. At all times after implementation of this Policy, ACME will maintain a current and accurate Notice of Artificial Intelligence Practices describing how ACME uses GAI tools and safeguards client confidential information. This

Notice should be clearly posted on the ACME website. Clients should be provided with this Notice as part their engagement documents, and within a reasonable time after we make any material changes to our policies and procedures for using GAI tools. No information related to client matters or confidential information should be processed in GAI tools prior to the client receiving this Notice.

- (b) Client Opt-Out Rights. Except as provided in Section 6(e), Clients have the right to restrict or prohibit the use of GAI tools in connection with their matters or to process their confidential information. A client may exercise this right at any time by providing written notice. Upon receipt of such notice, the client’s preferences should be clearly and prominently documented in the client file. All ACME Workforce members on the file should be notified of the client’s opt-out and take immediate steps to ensure that GAI tools are not used in any manner that violates the client’s expressed restrictions.

Accordingly, unless a client has opted out, members of the ACME Workforce may use Approved GAI Tools for the following purposes:

- i. De-Identified Processing. Approved GAI Tools may be used as a work assistant without inputting any personally identifiable or client confidential information. This could include posing hypothetical questions to an Approved GAI Tool to help generate a checklist for drafting documents.
  - ii. Non-Sensitive Confidential Processing. Approved GAI Tools may also be used to process client identifying or confidential information **other than Sensitive Personal Information as defined in the next section.** For example, a document may be uploaded to an Approved GAI Tool to support efficient review of that document, provided any Sensitive Personal Information has first been redacted.
- (c) Sensitive Personal Information. Prior to using an Approved GAI Tool to process Sensitive Personal Information, as defined below, ACME must obtain the client’s informed written consent using the procedure described in Section 6(d). For the purposes of this Policy, Sensitive Personal Information includes:

- Social security numbers or tax returns
- Driver’s license numbers or state identification card numbers
- Account, credit card, or debit card numbers
- Medical information, including mental health or substance abuse treatment records
- Health insurance information
- Unique biometric identifiers or biometric information (as defined in Illinois law)
- Passwords and security questions and answers used to access computer accounts
- Any other information meeting PIPA’s definition of “personal information,” even if separated from a first name or first initial in combination with last name

- (d) Informed Client Consent. Where client consent is required, it must be informed. The client must receive a clear explanation of the purpose of the processing, the type of data involved, the type of GAI tool to be used, the potential risks (including risks of disclosure or misuse), and the safeguards in place to protect the data. This information must be provided separately from other materials, and the client must be given the opportunity to ask questions before providing consent. Consent must be voluntary and may be revoked at any time and for any reason.
- i. Authority to Consent. The client may provide consent to process personal data that is (i) the personal data of the client or (ii) personal data of which the client is the lawful controller or processor. If the responsible attorney has reason to doubt the client’s authority to consent to the processing for the personal data provided, they must refrain from processing the data using GAI until appropriate authorization is confirmed.
  - ii. Discretionary Consents. The attorney responsible for any client or matter is free to require informed written consent for the use of Approved GAI Tools using criteria that is more restrictive than this Policy provides. If, in the professional judgment of the responsible attorney, informed written consent is prudent in any matter, then the responsible attorney’s judgment shall control.
- (e) System-Wide Processing. “*System-Wide Processing*” means using GAI systems in firm-wide administrative, security, or operational tools as part of standard functions, such as document management, email filtering, cybersecurity, or automated billing. These GAI tools are exempt from client opt-out or consent rights described above.
7. Implementation of Client and Project Level Restrictions. Prior to using Approved GAI Tools for any client or client project, the responsible attorney for the matter must complete an evaluation to determine whether any regulatory, contractual, or other specific obligations apply to the client or project. Approved GAI Tools may not be used unless such requirements are identified and complied with. For example:
- i. Client-Imposed Restrictions. Clients may include GAI-related restrictions in their agreements or engagement letters. As described above, clients may also file an opt-out request to limit or prohibit the use of GAI tools to process their data.
  - ii. Flow-Down Restrictions. Clients may be subject to GAI limitations that flow down to ACME, such as public-sector procurement rules (e.g. the California State GenAI Procurement Guidelines).
  - iii. Data Protection Requirements. Certain client data may be subject to heightened privacy or security obligations that require additional safeguards around GAI use, including but not limited to the CCPA, GDPR, or HIPAA.

- 8. Court and Regulatory Rules. Some courts or regulators may require the use of GAI tools to be disclosed, documented, or certified. These rules may require a party to: (i) identify which GAI tool was used in drafting a court filing; (ii) explain how the GAI tool was used in preparing court filings or regulated submissions; (iii) verify the accuracy of AI-generated content using non-GAI authoritative sources; and/or (iv) confirm that no confidential or proprietary information was disclosed to unauthorized parties. Accordingly, prior to using Approved GAI Tools to prepare any materials that will be used in a judicial or regulatory proceeding, the supervising attorney will confirm what GAI rules apply to that proceeding.
- 9. Data Minimization. Each ACME Workforce member must limit the retention of data in Approved GAI Tools to only what is reasonably necessary to support the project or matter for which the Approved GAI Tools are used. Approved GAI Tools should not be used as long-term storage or recordkeeping systems. For example, Workforce members should delete conversations, documents, prompts, instructions, memory functions, and other related data when the associated client matter is closed, or if no longer reasonably needed to manage that specific project or matter.
- 10. Education and Training. The ACME Managing Partner will coordinate education and training for all members of the ACME Workforce on the responsible use of artificial intelligence, including the requirements of this Policy. This training should include understanding ethical implications, data privacy and security risks, and the effective practical use of approved GAI tools and extensions.
- 11. Intellectual Property. The output of a Generative Artificial Intelligence tool may not be subject to intellectual property protection. Accordingly, Generative Artificial Intelligence output may not be incorporated into materials intended to have intellectual property protection without specific review and approval on a case-by-case basis. Accordingly, absent such review and approval, all work product intended to receive intellectual property protection must be original work produced by ACME Workforce members acting within the scope of their employment or engagement and not work product that is produced by a GAI tool.
- 12. Enhanced Periodic Review. As previously noted, the field of Artificial Intelligence is evolving rapidly. Accordingly, this Policy must be reviewed on a more frequent basis than provided in other ACME policies. The ACME Managing Partner is therefore directed to establish an Artificial Intelligence Review Committee and a policy review schedule that is appropriate to the speed at which this technology is evolving and the rate at which AI-related tools are adopted within ACME (and our clients and vendors).
- 13. Version Control. Any amendments or additions to this Policy shall be reflected in a new version and summarized in the attached Revision Management Log.

<b>Revision Management Log</b>		
Revision ID	Date	Brief Description
AI-100.1	*****	Initial Policy Adoption

## Appendix 5

### Sample Informed Client Consent Form

---

#### **Informed Consent for the Use of Generative Artificial Intelligence**

**Matter:** [Insert Matter Title]

**Client:** [Insert Client Name]

Acme Law, LLC may use Generative Artificial Intelligence (“GAI”) tools to support legal work such as document analysis, summarization, legal research, or drafting. These tools can improve efficiency and enhance the quality of legal services when used responsibly and with appropriate safeguards. In your matter, we believe it may be beneficial and appropriate to process certain sensitive personal information using GAI tools. Accordingly, we request your written consent to use GAI tools to process sensitive personal information related to your matter.

#### **Categories of Sensitive Personal Information to be Processed**

Absent additional written consent, we will only use GAI tools to process the following categories of Sensitive Personal Information:

- Social Security numbers
- Driver’s license or state ID numbers
- Financial account numbers or payment card data
- Medical or health insurance information
- Other information covered by the Illinois Personal Information Protection Act

#### **Purpose of Processing**

We will only process sensitive personal information using GAI tools if it is directly relevant to the legal services we are providing and necessary to achieve a meaningful benefit, such as faster document review, clearer summarization, or improved accuracy in analysis. Due to the volume of documents that must be reviewed in your matter, we believe the use of GAI tools will improve accuracy and reduce the time needed to perform our work.

#### **GAI Tools to be Used**

If you consent, we will only use business-class GAI tools which are subject to appropriate privacy and security assurances. The specific GAI tools used by ACME Law, LLC are available in our Notice of Artificial Intelligence Practices that is updated no less than quarterly.

**Client Consent**

I have read and understand this form and ACME Law, LLC’s Notice of Artificial Intelligence Practices. I understand the nature and purpose of this request, and I have been given the opportunity to discuss any questions or concerns I may have with individuals who are knowledgeable about the specific GAI tools that will be used to process my sensitive personal information.

I understand that I may revoke this consent at any time and for any reason by using the contact information provided in ACME Law, LLC’s Notice of Artificial Intelligence Practices. I also understand that my revocation will only be effective for uses of my personal information after the effective date of my revocation, and that my revocation will not apply to the use of GAI for system-wide processing within ACME Law, LLC’s network and computer systems.

Accordingly, I consent to Acme Law, LLC’s use of GAI tools as described above.

\_\_\_\_\_

Dated: \_\_\_\_\_

**Appendix 6**  
**Cybersecurity Information Sheet (“CIS”)**  
**Deploying AI Systems Securely: Best Practices for**  
**Deploying Secure and Resilient AI Systems**

# Joint Cybersecurity Information

TLP:CLEAR



Communications Security Establishment Canada

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada

Centre canadien pour la cybersécurité



National Cyber Security Centre  
a part of GCHQ

## Deploying AI Systems Securely

*Best Practices for Deploying Secure and Resilient AI Systems*

### Executive summary

Deploying artificial intelligence (AI) systems securely requires careful setup and configuration that depends on the complexity of the AI system, the resources required (e.g., funding, technical expertise), and the infrastructure used (i.e., on premises, cloud, or hybrid). This report expands upon the 'secure deployment' and 'secure operation and maintenance' sections of the [Guidelines for secure AI system development](#) and incorporates mitigation considerations from [Engaging with Artificial Intelligence \(AI\)](#). It is for organizations deploying and operating AI systems designed and developed by another entity. The best practices may not be applicable to all environments, so the mitigations should be adapted to specific use cases and threat profiles. [1], [2]

AI security is a rapidly evolving area of research. As agencies, industry, and academia discover potential weaknesses in AI technology and techniques to exploit them, organizations will need to update their AI systems to address the changing risks, in addition to applying traditional IT best practices to AI systems.

This report was authored by the U.S. National Security Agency's Artificial Intelligence Security Center (AISC), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK). The goals of the AISC and the report are to:

1. Improve the confidentiality, integrity, and availability of AI systems;
2. Assure that known cybersecurity vulnerabilities in AI systems are appropriately mitigated; and
3. Provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

*This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more on the Traffic Light Protocol, see [cisa.gov/ttp/](https://cisa.gov/ttp/).*

TLP:CLEAR

## Scope and audience

The term AI systems throughout this report refers to machine learning (ML) based artificial intelligence (AI) systems.

These best practices are most applicable to organizations deploying and operating externally developed AI systems on premises or in private cloud environments, especially those in high-threat, high-value environments. They are not applicable for organizations who are not deploying AI systems themselves and instead are leveraging AI systems deployed by others.

Not all of the guidelines will be directly applicable to all organizations or environments. The level of sophistication and the methods of attack will vary depending on the adversary targeting the AI system, so organizations should consider the guidance alongside their use cases and threat profile.

See [Guidelines for secure AI system development](#) for design and development aspects of AI systems. [1]

## Introduction

The rapid adoption, deployment, and use of AI capabilities can make them highly valuable targets for malicious cyber actors. Actors, who have historically used data theft of sensitive information and intellectual property to advance their interests, may seek to co-opt deployed AI systems and apply them to malicious ends.

Malicious actors targeting AI systems may use attack vectors unique to AI systems, as well as standard techniques used against traditional IT. Due to the large variety of attack vectors, defenses need to be diverse and comprehensive. Advanced malicious actors often combine multiple vectors to execute operations that are more complex. Such combinations can more effectively penetrate layered defenses.

Organizations should consider the following best practices to secure the deployment environment, continuously protect the AI system, and securely operate and maintain the AI system.

The best practices below align with the cross-sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on

existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's [Cross-Sector Cybersecurity Performance Goals](#) for more information on the CPGs, including additional recommended baseline protections.

## Secure the deployment environment

Organizations typically deploy AI systems within existing IT infrastructure. Before deployment, they should ensure that the IT environment applies [sound security principles](#), such as robust governance, a well-designed architecture, and secure configurations. For example, ensure that the person responsible and accountable for AI system cybersecurity is the same person responsible and accountable for the organization's cybersecurity in general [[CPG 1.B](#)].

The security best practices and requirements for IT environments apply to AI systems, too. The following best practices are particularly important to apply to the AI systems and the IT environments the organization deploys them in.

### *Manage deployment environment governance*

- If an organization outside of IT is deploying or operating the AI system, work with the IT service department to identify the deployment environment and confirm it meets the organization's IT standards.
  - Understand the organization's risk level and ensure that the AI system and its use is within the organization's risk tolerance overall and within the risk tolerance for the specific IT environment hosting the AI system. Assess and document applicable threats, potential impacts, and risk acceptance. [3], [4]
  - Identify the roles and responsibilities for each stakeholder along with how they are accountable for fulfilling them; identifying these stakeholders is especially important should the organization manage their IT environment separately from their AI system.
  - Identify the IT environment's security boundaries and how the AI system fits within them.
- Require the primary developer of the AI system to provide a threat model for their system.

- The AI system deployment team should leverage the threat model as a guide to implement security best practices, assess potential threats, and plan mitigations. [5], [6]
- Consider deployment environment security requirements when developing contracts for AI system products or services.
- Promote a collaborative culture for all parties involved, including the data science, infrastructure, and cybersecurity teams in particular, to allow for teams to voice any risks or concerns and for the organization to address them appropriately.

## ***Ensure a robust deployment environment architecture***

- Establish security protections for the boundaries between the IT environment and the AI system [[CPG 2.F](#)].
- Identify and address blind spots in boundary protections and other security-relevant areas in the AI system the threat model identifies. For example, ensure the use of an access control system for the AI model weights and limit access to a set of privileged users with two-person control (TPC) and two-person integrity (TPI) [[CPG 2.E](#)].
- Identify and protect all proprietary data sources the organization will use in AI model training or fine-tuning. Examine the list of data sources, when available, for models trained by others. Maintaining a catalog of trusted and valid data sources will help protect against potential data poisoning or backdoor attacks. For data acquired from third parties, consider contractual or service level agreement (SLA) stipulations as recommended by [CPG 1.G](#) and [CPG 1.H](#).
- Apply secure by design principles and Zero Trust (ZT) frameworks to the architecture to manage risks to and from the AI system. [7], [8], [9]

## ***Harden deployment environment configurations***

- Apply existing security best practices to the deployment environment. This includes sandboxing the environment running ML models within hardened containers or virtual machines (VMs) [[CPG 2.E](#)], monitoring the network [[CPG 2.T](#)], configuring firewalls with allow lists [[CPG 2.F](#)], and other best practices, such as those in [NSA's Top Ten Cloud Mitigation Strategies](#) for cloud deployments.
- Review hardware vendor guidance and notifications (e.g., for GPUs, CPUs, memory) and apply software patches and updates to minimize the risk of exploitation of vulnerabilities, preferably via the Common Security Advisory Framework (CSAF). [10]

- Secure sensitive AI information (e.g., AI model weights, outputs, and logs) by encrypting the data at rest, and store encryption keys in a hardware security module (HSM) for later on-demand decryption [[CPG 2.L](#)].
- Implement strong authentication mechanisms, access controls, and secure communication protocols, such as by using the latest version of Transport Layer Security (TLS) to encrypt data in transit [[CPG 2.K](#)].
- Ensure the use of [phishing-resistant multifactor authentication](#) (MFA) for access to information and services. [2] Monitor for and respond to fraudulent authentication attempts [[CPG 2.H](#)]. [11]
- Understand and mitigate how malicious actors exploit weak security controls by following the mitigations in [Weak Security Controls and Practices Routinely Exploited for Initial Access](#).

## ***Protect deployment networks from threats***

Adopt a ZT mindset, which assumes a breach is inevitable or has already occurred. Implement detection and response capabilities, enabling quick identification and containment of compromises. [8], [9]

- Use well-tested, high-performing cybersecurity solutions to identify attempts to gain unauthorized access efficiently and enhance the speed and accuracy of incident assessments [[CPG 2.G](#)].
- Integrate an incident detection system to help prioritize incidents [[CPG 3.A](#)]. Also integrate a means to immediately block access by users suspected of being malicious or to disconnect all inbound connections to the AI models and systems in case of a major incident when a quick response is warranted.

## **Continuously protect the AI system**

Models are software, and, like all other software, may have vulnerabilities, other weaknesses, or malicious code or properties.

### ***Validate the AI system before and during use***

- Use cryptographic methods, digital signatures, and checksums to confirm each artifact's origin and integrity (e.g., encrypt safetensors to protect their integrity and confidentiality), protecting sensitive information from unauthorized access during AI processes. [14]

- Create hashes and encrypted copies of each release of the AI model and system for archival in a tamper-proof location, storing the hash values and/or encryption keys inside a secure vault or HSM to prevent access to both the encryption keys and the encrypted data and model at the same location. [1]
- Store all forms of code (e.g., source code, executable code, infrastructure as code) and artifacts (e.g., models, parameters, configurations, data, tests) in a version control system with proper access controls to ensure only validated code is used and any changes are tracked. [1]
- Thoroughly test the AI model for robustness, accuracy, and potential vulnerabilities after modification. Apply techniques, such as adversarial testing, to evaluate the model's resilience against compromise attempts. [4]
- Prepare for automated rollbacks and use advanced deployments with a human-in-the-loop as a failsafe to boost reliability, efficiency, and enable continuous delivery for AI systems. In the context of an AI system, rollback capabilities ensure that if a new model or update introduces problems or if the AI system is compromised, the organization can quickly revert to the last known good state to minimize the impact on users.
- Evaluate and secure the supply chain for any external AI models and data, making sure they adhere to organizational standards and risk management policies, and preferring ones developed according to secure by design principles. Make sure that the risks are understood and accepted for parts of the supply chain that cannot adhere to organizational standards and policies. [1], [7]
- Do not run models right away in the enterprise environment. Carefully inspect models, especially imported pre-trained models, inside a secure development zone prior to considering them for tuning, training, and deployment. Use organization-approved AI-specific scanners, if and when available, for the detection of potential malicious code to assure model validity before deployment.
- Consider automating detection, analysis, and response capabilities, making IT and security teams more efficient by giving them insights that enable quick and targeted reactions to potential cyber incidents. Perform continuous scans of AI models and their hosting IT environments to identify possible tampering.
  - When considering whether to use other AI capabilities to make automation more efficient, carefully weigh the risks and benefits, and ensure there is a human-in-the-loop where needed.

## ***Secure exposed APIs***

- If the AI system exposes application programming interfaces (APIs), secure them by implementing authentication and authorization mechanisms for API access. Use secure protocols, such as HTTPS with encryption and authentication [CPG [2.C](#), [2.D](#), [2.G](#), [2.H](#)]. [1]
- Implement validation and sanitization protocols for all input data to reduce the risk of undesired, suspicious, incompatible, or malicious input being passed to the AI system (e.g., prompt injection attacks). [1]

## ***Actively monitor model behavior***

- Collect logs to cover inputs, outputs, intermediate states, and errors; automate alerts and triggers [CPG [2.T](#)].
- Monitor the model's architecture and configuration settings for any unauthorized changes or unexpected modifications that might compromise the model's performance or security. [1]
- Monitor for attempts to access or elicit data from the AI model or aggregate inference responses. [1]

## ***Protect model weights***

- Harden interfaces for accessing model weights to increase the effort it would take for an adversary to exfiltrate the weights. For example, ensure APIs return only the minimal data required for the task to inhibit model inversion.
- Implement hardware protections for model weight storage as feasible. For example, disable hardware communication capabilities that are not needed and protect against emanation or side channel techniques.
- Aggressively isolate weight storage. For example, store model weights in a protected storage vault, in a highly restricted zone (HRZ) (i.e., a separate dedicated enclave), or using an HSM [CPG [2.L](#)]. [12]

## **Secure AI operation and maintenance**

Follow organization-approved IT processes and procedures to deploy the AI system in an approved manner, ensuring the following controls are implemented.

## ***Enforce strict access controls***

- Prevent unauthorized access or tampering with the AI model. Apply role-based access controls (RBAC), or preferably attribute-based access controls (ABAC) where feasible, to limit access to authorized personnel only.
  - Distinguish between users and administrators. Require MFA and privileged access workstations (PAWs) for administrative access [[CPG 2.H](#)].

## ***Ensure user awareness and training***

Educate users, administrators, and developers about security best practices, such as strong password management, phishing prevention, and secure data handling. Promote a security-aware culture to minimize the risk of human error. If possible, use a credential management system to limit, manage, and monitor credential use to minimize risks further [[CPG 2.I](#)].

## ***Conduct audits and penetration testing***

- Engage external security experts to conduct audits and penetration testing on ready-to-deploy AI systems. This helps identify vulnerabilities and weaknesses that may have been overlooked internally. [13], [15]

## ***Implement robust logging and monitoring***

- Monitor the system's behavior, inputs, and outputs with robust monitoring and logging mechanisms to detect any abnormal behavior or potential security incidents [[CPG 3.A](#)]. [16] Watch for data drift or high frequency or repetitive inputs (as these could be signs of model compromise or automated compromise attempts). [17]
- Establish alert systems to notify administrators of potential oracle-style adversarial compromise attempts, security breaches, or anomalies. Timely detection and response to cyber incidents are critical in safeguarding AI systems. [18]

## ***Update and patch regularly***

- When updating the model to a new/different version, run a full evaluation to ensure that accuracy, performance, and security tests are within acceptable limits before redeploying.

## ***Prepare for high availability (HA) and disaster recovery (DR)***

- Use an immutable backup storage system, depending on the requirements of the system, to ensure that every object, especially log data, is immutable and cannot be changed [[CPG 2.R](#)]. [2]

## ***Plan secure delete capabilities***

- Perform autonomous and irretrievable deletion of components, such as training and validation models or cryptographic keys, without any retention or remnants at the completion of any process where data and models are exposed or accessible. [19]

## **Conclusion**

The authoring agencies advise organizations deploying AI systems to implement robust security measures capable of both preventing theft of sensitive data and mitigating misuse of AI systems. For example, model weights, the learnable parameters of a deep neural network, are a particularly critical component to protect. They uniquely represent the result of many costly and challenging prerequisites for training advanced AI models, including significant compute resources; collected, processed, and potentially sensitive training data; and algorithmic optimizations.

AI systems are software systems. As such, deploying organizations should prefer systems that are secure by design, where the designer and developer of the AI system takes an active interest in the positive security outcomes for the system once in operation. [7]

Although comprehensive implementation of security measures for all relevant attack vectors is necessary to avoid significant security gaps, and best practices will change as the AI field and techniques evolve, the following summarizes some particularly important measures:

- Conduct ongoing compromise assessments on all devices where privileged access is used or critical services are performed.
- Harden and update the IT deployment environment.
- Review the source of AI models and supply chain security.
- Validate the AI system before deployment.
- Enforce strict access controls and API security for the AI system, employing the concepts of least privilege and defense-in-depth.

- Use robust logging, monitoring, and user and entity behavior analytics (UEBA) to identify insider threats and other malicious activities.
- Limit and protect access to the model weights, as they are the essence of the AI system.
- Maintain awareness of current and emerging threats, especially in the rapidly evolving AI field, and ensure the organization's AI systems are hardened to avoid security gaps and vulnerabilities.

In the end, securing an AI system involves an ongoing process of identifying risks, implementing appropriate mitigations, and monitoring for issues. By taking the steps outlined in this report to secure the deployment and operation of AI systems, an organization can significantly reduce the risks involved. These steps help protect the organization's intellectual property, models, and data from theft or misuse.

Implementing good security practices from the start will set the organization on the right path for deploying AI systems successfully.

## Works cited

- [1] National Cyber Security Centre et al. Guidelines for secure AI system development. 2023. <https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf>
- [2] Australian Signals Directorate et al. Engaging with Artificial Intelligence (AI). 2024. <https://www.cyber.gov.au/sites/default/files/2024-01/Engaging%20with%20Artificial%20Intelligence%20%28AI%29.pdf>
- [3] MITRE. ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) Matrix version 4.0.0. 2024. <https://atlas.mitre.org/matrices/ATLAS>
- [4] National Institute of Standards and Technology. AI Risk Management Framework 1.0. 2023. <https://www.nist.gov/itl/ai-risk-management-framework>
- [5] The Open Worldwide Application Security Project (OWASP®). LLM AI Cybersecurity & Governance Checklist. 2024. [https://owasp.org/www-project-top-10-for-large-language-model-applications/llm-top-10-governance-doc/LLM\\_AI\\_Security\\_and\\_Governance\\_Checklist-v1.pdf](https://owasp.org/www-project-top-10-for-large-language-model-applications/llm-top-10-governance-doc/LLM_AI_Security_and_Governance_Checklist-v1.pdf)
- [6] The Open Worldwide Application Security Project (OWASP®). OWASP Machine Learning Security Top Ten Security Risks. 2023. <https://owasp.org/www-project-machine-learning-security-top-10/>
- [7] Cybersecurity and Infrastructure Security Agency. Secure by Design. 2023. <https://www.cisa.gov/securebydesign>
- [8] National Security Agency. Embracing a Zero Trust Security Model. 2021. [https://media.defense.gov/2021/Feb/25/2002588479/-1-/1/0/CSI\\_EMBRACING\\_ZT\\_SECURITY\\_MODEL\\_UOO115131-21.PDF](https://media.defense.gov/2021/Feb/25/2002588479/-1-/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF)
- [9] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. 2022. <https://www.cisa.gov/zero-trust-maturity-model>
- [10] Cybersecurity and Infrastructure Security Agency. Transforming the Vulnerability Management Landscape. 2022. <https://www.cisa.gov/news-events/news/transforming-vulnerability-management-landscape>

- [11] Cybersecurity and Infrastructure Security Agency. Implementing Phishing-Resistant MFA. 2022. <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
- [12] Canadian Centre for Cyber Security. Baseline security requirements for network security zones Ver. 2.0 (ITSP.80.022). 2021. <https://www.cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022>
- [13] Ji, Jessica. What Does AI Red-Teaming Actually Mean? 2023. <https://cset.georgetown.edu/article/what-does-ai-red-teaming-actually-mean/>
- [14] Hugging Face GitHub. Safetensors. 2024. <https://github.com/huggingface/safetensors>.
- [15] Michael Feffer, Anusha Sinha, Zachary C. Lipton, Hoda Heidari. Red-Teaming for Generative AI: Silver Bullet or Security Theater? 2024. <https://arxiv.org/abs/2401.15897>
- [16] Google. Google's Secure AI Framework (SAIF). 2023. <https://safety.google/cybersecurity-advancements/saif/>
- [17] Government Accountability Office (GAO). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. 2021. <https://www.gao.gov/assets/gao-21-519sp.pdf>
- [18] RiskInsight. Attacking AI? A real-life example!. 2023. <https://riskinsight-wavestone.com/en/2023/06/attacking-ai-a-real-life-example>
- [19] National Cyber Security Centre. Principles for the security of machine learning. 2022. <https://www.ncsc.gov.uk/files/Principles-for-the-security-of-machine-learning.pdf>

## ***Disclaimer of endorsement***

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## ***Purpose***

This document was developed in furtherance of the authoring organizations' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

## ***Contact***

### **U.S. organizations:**

NSA Cybersecurity Report Feedback: [CybersecurityReports@nsa.gov](mailto:CybersecurityReports@nsa.gov)

NSA General Cybersecurity Inquiries or Customer Requests: [Cybersecurity\\_Requests@nsa.gov](mailto:Cybersecurity_Requests@nsa.gov)

Defense Industrial Base Inquiries and Cybersecurity Services: [DIB\\_Defense@cyber.nsa.gov](mailto:DIB_Defense@cyber.nsa.gov)

NSA Media Inquiries / Press Desk: 443-634-0721, [MediaRelations@nsa.gov](mailto:MediaRelations@nsa.gov)

Report incidents and anomalous activity to CISA 24/7 Operations Center at [report@cisa.gov](mailto:report@cisa.gov) or (888) 282-0870 and/or to the FBI via your [local FBI field office](#).

**Australian organizations:** For more information or to report a cybersecurity incident, visit [cyber.gov.au](https://cyber.gov.au) or call 1300 292 371 (1300 CYBER1).

**Canadian organizations:** For more information contact the Cyber Centre at [contact@cyber.gc.ca](mailto:contact@cyber.gc.ca) or report a cyber security incident to our portal at <https://www.cyber.gc.ca/en/incident-management>.

**New Zealand organizations:** Report cyber security incidents to [incidents@ncsc.govt.nz](mailto:incidents@ncsc.govt.nz) or call 04 498 7654.

**United Kingdom organizations:** Report a significant cyber security incident at [ncsc.gov.uk/report-an-incident](https://ncsc.gov.uk/report-an-incident) (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

# ARDC



ATTORNEY  
REGISTRATION  
& DISCIPLINARY  
COMMISSION

One Prudential Plaza  
130 East Randolph Drive  
Suite 1500  
Chicago, Illinois 60601-6219  
312.565.2600

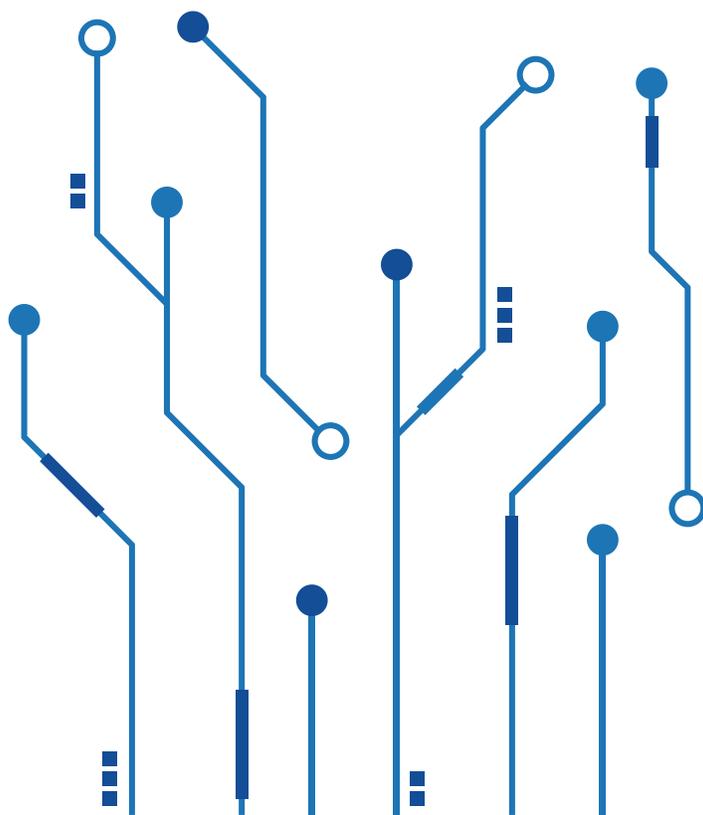
3161 West White Oaks Drive  
Suite 301  
Springfield, Illinois 62704  
217.546.3523

[www.iardc.org](http://www.iardc.org)



# ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

EFFECTIVE JANUARY 1, 2025



Embracing the advancements of artificial intelligence (AI), the Illinois Supreme Court remains steadfast in its commitment to upholding the highest ethical standards in the administration of justice. We acknowledge the rapid development of generative AI technologies capable of producing human-like text, images, video, audio, and other content. The integration of AI with the courts is increasingly pervasive, offering potential efficiencies and improved access to justice. However, it also raises critical concerns about authenticity, accuracy, bias, and the integrity of court filings, proceedings, evidence, and decisions. Understanding the capabilities and limitations of AI technology is essential for the Illinois Judicial Branch.

The Illinois Courts will be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice. Unsubstantiated or deliberately misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making will not be tolerated.

The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.

The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations. Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

This policy reflects the Illinois Supreme Court's commitment to upholding foundational principles while exploring the potential benefits of new AI technologies in a dynamic landscape. The Court will regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice. **Judges remain ultimately responsible for their decisions, irrespective of technological advancements.**

The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice. To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI.





[LAURA BAGBY](#) | [FUTURE LAW](#) | JANUARY 10, 2025

# Illinois Supreme Court Releases Policy on AI in State Courts



In December, the Illinois Supreme Court [announced a policy](#) governing the use of artificial intelligence (AI) in Illinois courts.

The [policy says that](#): “The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.”

The policy took effect on January 1, 2025.

## Studying AI's impact on state courts

The policy follows the Court's approval of a report from the Illinois Judicial Conference's Task Force on Artificial Intelligence (IJC AI Task Force), which was created to recommend how the Illinois Judicial Branch should use and regulate AI. This included exploring how AI impacts policy, education, and customer service, as well as potential amendments to court rules.

The IJC AI Task Force was co-chaired by Williamson County Judge Jeffrey A. Goffinet and 17th Judicial Circuit Trial Court Administrator Thomas R. Jakeway and [included the Commission on Professionalism's](#) Chief Counsel Mark C. Palmer.

"Courts must do everything they can to keep up with this rapidly changing technology," Chief Justice Mary Jane Theis [said in the press release](#). "This policy recognizes that while AI use continues to grow, our current rules are sufficient to govern its use. However, there will be challenges as these systems evolve and the Court will regularly reassess those rules and this policy."

Illinois is one of the first states to release guidelines on the use of AI in state courts.

## Illinois Supreme Court AI Policy

The full [Illinois Supreme Court Policy on Artificial Intelligence](#) is below:

Embracing the advancements of artificial intelligence (AI), the Illinois Supreme Court remains steadfast in its commitment to upholding the highest ethical standards in the administration of justice. We acknowledge the rapid development of generative AI technologies capable of producing human-like text, images, video, audio, and other content. The integration of AI with the courts is increasingly pervasive, offering potential efficiencies and improved access to justice. However, it also raises critical concerns about authenticity, accuracy, bias, and the integrity of court filings, proceedings, evidence, and decisions. Understanding the capabilities and limitations of AI technology is essential for the Illinois Judicial Branch.

The Illinois Courts will be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice. Unsubstantiated or deliberately

misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making will not be tolerated.

The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.

The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations. Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

This policy reflects the Illinois Supreme Court's commitment to upholding foundational principles while exploring the potential benefits of new AI technologies in a dynamic landscape. The Court will regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice. **Judges remain ultimately responsible for their decisions, irrespective of technological advancements.**

The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice. To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI.

###

A judicial reference sheet ("bench card") to support judges [can be found here](#).

Staying up to date on issues impacting the legal profession is vital to your success. [Subscribe here](#) to get the Commission's weekly news delivered to your inbox.

“ [Commission on Professionalism's Most-Read Articles of 2024](#) ”

“ [How Lawyers Can Overcome Fear and Embrace AI in 2025](#) ”

“ [Crafting Influence: The Role of Language and AI in Legal Advocacy](#) ”

How useful was this post?

Click on a star to rate it!



# Judiciary AI Rule Draws Fire As Judges Get Deepfakes Survey

By **Jeff Overley**

Law360 (January 15, 2026, 8:32 PM EST) -- Federal judiciary policymakers heard extensive concerns Thursday regarding high-profile plans to formally screen evidence generated with artificial intelligence, and they set the stage for more feedback by preparing an AI survey for every federal trial judge.

The concerns came from a small yet disparate set of witnesses during the first of two public hearings before the judiciary's Advisory Committee on Evidence Rules, which has **proposed standards** for the introduction of so-called machine-generated evidence without an expert witness.

Three of Thursday's five witnesses on the AI topic have current or past ties to advocacy group Lawyers for Civil Justice, whose members include scores of BigLaw firms and some of the world's largest corporations. A technology entrepreneur and a veteran plaintiffs attorney who also spoke largely echoed the witnesses from big business and the defense bar.

"You might never have thought you'd hear a pure plaintiffs lawyer say they agree with LCJ, but I do agree with LCJ's concern ... that the new rule may create a pathway" for easier admission of AI evidence, said Jeannine M. Kenney, a class action specialist at Hausfeld LLP, during Thursday's videoconference hearing.

Several witnesses testified Thursday that the effort, while commendable, seems premature. The committee's chair, U.S. District Judge Jesse M. Furman, has acknowledged that critique while also stressing AI's swift evolution and the sluggish pace of judiciary policymaking. He reiterated those points Thursday, citing "the tension between how fast technology is moving and how slow the rulemaking process is."

At issue is **draft Rule 707**, which advisers to the Judicial Conference of the United States **released last year** for a public comment period that will include another hearing Jan. 29 before wrapping up Feb. 16. The brevity of the draft rule, which contains only about 50 words, is in stark contrast with the voluminous responses, such as a nearly 5,000-word letter that the LCJ submitted this month.

Proposed Rule 707, which cites **Federal Rule of Evidence 702's**  four-prong test to ensure human experts are reliable, says: "When machine-generated evidence is offered without an expert witness and would be subject to Rule 702 if testified to by a witness, the court may admit the evidence only if it satisfies the requirements of Rule 702(a)-(d). This rule does not apply to the output of simple scientific instruments."

Alex Dahl, general counsel of the LCJ, recommended several revisions Thursday, including terminology akin to "machine opinions." That change would avoid overlap with simple technology — such as the Microsoft Teams platform on which Thursday's hearing was held — that routinely generates data outside the true ambit of Rule 707, Dahl said.

Making that change also "would allow you to delete the sentence about 'simple scientific instruments,'" Dahl said, adding that the nature of those instruments "is going to be a lightning rod" for courtroom disputes if the sentence is preserved.

Thomas Y. Allman, a onetime LCJ official and former general counsel of BASF Corp., echoed other witnesses by urging a decoupling of Rules 702 and 707, and more specificity in Rule 707 regarding

AI's technical aspects. Rule 707's vision of AI evidence being presented without an expert witness might be a largely theoretical problem, he added.

"If they don't come with an expert, they're a fool," Allman said. "Because on cross-examination, they're going to be taken apart when they cannot explain how [their] system works."

There would be upsides to greater specificity in Rule 707, Judge Furman said Thursday, but simply utilizing Rule 702 has considerable benefits, because it's widely understood. Committee members, he said, have felt that the "disadvantages of the need to translate [Rule 702] for machines were outweighed by the advantages of familiarity."

Robert L. Levy, executive counsel at ExxonMobil Corp. and treasurer of the LCJ, nonetheless testified later Thursday that "a standalone rule on this issue is the better [approach] because of the complexity of trying to utilize the 702 construct." But Levy simultaneously floated the prospect of a larger AI rule that also incorporates the committee's idea for Rule 901(c), a conceptual provision to ferret out phony audio clips or videos known as "deepfakes."

Judge Furman, who **recently announced** that the Federal Judicial Center would be assisting with a nationwide survey of judges' experiences with deepfakes, replied Thursday that the "survey is going out to every federal trial judge in the country today to solicit their experience and views on that."

Law360 on Thursday requested a copy of the survey from the FJC and Judge Furman, but did not immediately receive a response.

The committee's **interest in the deepfakes issue** represents a modest reversal; the topic was initially **put on the back-burner** amid suggestions that fears of manipulated recordings were overblown. Similarly, there was some discussion Thursday about the dearth of court cases involving machine-generated evidence that turns out to be shoddy.

One of the few precedents that came up was a 2024 decision from New York state court in a case called **Matter of Weber** . In that case, an expert witness utilized the AI chatbot Microsoft Copilot, but he "could not recall what input or prompt he used to assist him," according to the decision.

The judge in the case wrote that he entered relevant numbers into Copilot and inquired about its reliability, to which the chatbot replied, "I do my best to be as reliable as possible. However, I'm also programmed to advise checking with experts for critical issues. Always good to have a second opinion!" And when asked specifically about its reliability for legal purposes, the chatbot replied, "I can provide accurate info, but it should always be verified by experts and accompanied by professional evaluations before being used in court."

--Editing by Marygrace Anderson.



Advertisement

ARTIFICIAL INTELLIGENCE

DOUBLE DOWN

## Lawyer Gets Caught Using AI in Court, Responds in the Worst Possible Way

Not making a great case for yourself, pal.



By [Frank Landymore](#) / Published **Oct 15, 2025 2:10 PM EDT**

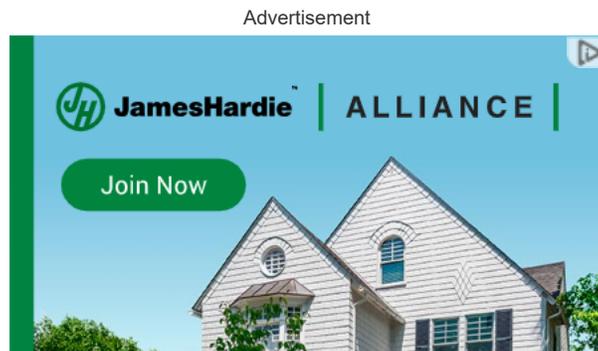


Getty / Futurism

What is it with lawyers and AI? We don't know, but it feels like an inordinate number of them keep screwing up with AI tools,

apparently never learning from their colleagues who get publicly crucified for making the same mistake.

But this latest blunder from a New York attorney, in a lawsuit centered on a disputed loan, takes the cake. As [404 Media reports](#), after getting caught using AI by leaving in hallucinated quotes and citations in his court filings, defense lawyer Michael Fourte then submitted a brief explaining his AI usage — which was *also* written with a large language model.



Needless to say, the judge was not amused.

“In other words, counsel relied upon unvetted AI — in his telling, via inadequately supervised colleagues — to defend his use of unvetted AI,” wrote New York Supreme Court judge Joel Cohen [in a decision filed earlier this month](#).

“This case adds yet another unfortunate chapter to the story of artificial intelligence misuse in the legal profession,” the judge further lamented.

Perhaps one of the reasons that we keep hearing about these completely avoidable catastrophes is that catching your opponent even making a single mistake using an AI tool is an easy way to gain an upper hand in court, so everyone's on the lookout for them.

That's what happened here: it was the plaintiff's legal team that first caught the mistakes, which included inaccurate or completely made up citations and quotations. The plaintiffs then filed a request for the judge to sanction Fourte, which is when he committed the legal equivalent of shoving a stick between the spokes of your bike wheel: he used AI again.

In his opposition to the sanctions motion, Fourte's submitted document contained more than double the amount of made-up or erroneous citations as last time, an astonished-sounding Cohen wrote.

Advertisement



His explanation was also pretty unsatisfactory. Fourte neither admitted nor denied the use of AI, wrote judge Cohen, but instead tried to pass off the botched citations as merely “innocuous paraphrases of accurate legal principles.”

Somehow, it gets worse. After the plaintiffs flagged the new wave of errors in Fourte's opposition to the sanctions motion, the defense lawyer — who by now was presumably sweating more than a character in a Spaghetti Western — then strongly implied that AI wasn't used at all, complaining that the plaintiffs provided “no affidavit, forensic analysis, or admission” confirming the use of the tech. When he had an opportunity to set the record straight during oral arguments in court, Fourte further insisted that the the “cases are not fabricated at all,” the judge noted.

Eventually, though, he cracked. After getting further grilled on how a completely made-up court case ended up in his filings, Fourte admitted he “did use AI.” He also, in practically the same breath, said he took “full responsibility” for the AI-generated nonsense — but also tried to pass off some of the blame on some additional staff he'd brought on the case. Classic.

Later, Fourte “muddled those statements of contrition,” the judge mused, by saying, “I never said I didn't use AI. I said that I didn't use unvetted AI.”

Advertisement



To which the judge called BS. “If you are including citations that don’t exist, there’s only one explanation for that. It’s that AI gave you cites and you didn’t check them,” Cohen responded to Fourte’s pleas. “That’s the definition of unvetted AI.”

After all the back and forth, Judge Cohen granted the plaintiff’s motion for sanctions.

Fourte declined 404’s request for comment. “As this matter remains before the Court, and out of respect for the process and client confidentiality, we will not comment on case specifics,” he told the outlet. “We have addressed the issue directly with the Court and implemented enhanced verification and supervision protocols. We have no further comment at this time.”

While his case seems especially egregious, Fourte is definitely not alone. Dozens of other lawyers have been caught using AI for largely the same reason: submitting erroneous or made up case law. Some used public chatbots like ChatGPT, but others used AI tools special-built for law, illustrating how fundamentally error-prone the tech remains.

One of the biggest firms caught in an AI scandal is Morgan & Morgan, which rushed out a panicked company-wide email after two of its lawyers faced sanctions for citing AI hallucinations earlier this year. Judges, meanwhile, have done their darndest to make an example out of lawyers careless enough to rely on the word of an LLM — but clearly, this latest case shows, not everyone’s getting the memo.



**More on AI:** [Top US Army General Says He's Letting ChatGPT Make Decisions to Make Military Decisions](#)

---



**Frank Landymore**  
**Contributing Writer**

I'm a tech and science correspondent for Futurism, where I'm particularly interested in astrophysics, the business and ethics of artificial intelligence and automation, and the environment.

---

Advertisement

MOST POPULAR

---

A Man Bought Meta's AI Glasses, and Ended Up Wandering the Desert Searching for Aliens to Abduct Him

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF OKLAHOMA**

**FILED**

OCT 22 2025

RONNIE HACKLER  
Clerk, U.S. District Court

By \_\_\_\_\_  
Deputy Clerk

SUZANNA and ROGER MATTOX, )

)

Plaintiffs, )

)

v. )

)

PRODUCT INNOVATIONS RESEARCH, )

)

LLC d/b/a SUNEVOLUTIONS; COSWAY )

)

COMPANY, INC.; and JOHN DOES 1-3, )

)

Defendants. )

Case No. 6:24-cv-235-JAR

**ORDER**

*“Trust, but verify.”*

— President Ronald Reagan, White House Press Conference (Dec. 16, 1987)

**I. INTRODUCTION**

This ruling is not about technology. It is about trust. Justice is built on language, and language draws its power from the hearts and minds that create it. Words alone are empty until filled with human conviction. The same is true of every pleading filed before this Court. Generative technology can produce words, but it cannot give them belief. It cannot attach courage, sincerity, truth, or responsibility to what it writes. That remains the sacred duty of the lawyer who signs the page.

Across eleven (11) pleadings, that duty was forgotten. As outlined below, Plaintiffs’ counsel submitted pleadings containing fabricated case citations, erroneous citations, quotations of nonexistent law, and misstatements of law. The

filings ranged from summary-judgment briefing, to motions in limine, and even a sanctions motion. The pattern was not inadvertent, and it was not harmless. The Court values trust among advocates, but trust must be earned through verification. In this case, filings were trusted, but never verified, and the results speak for themselves.

After reviewing the record, conducting two show-cause hearings, and considering the affidavits, testimony, and argument of counsel, the Court finds that the use of generative artificial intelligence in the preparation of these pleadings violated both Rule 11(b) of the Federal Rules of Civil Procedure and this Court's *AI Guidelines on Generative AI Disclosure and Certification*<sup>1</sup>.

The integrity of judicial proceedings depends on the authenticity of what is filed. This case demonstrates the cost of neglecting that obligation.

## II. BACKGROUND

### A. Procedural

This case was removed from state court on July 10, 2024. Over the following year, multiple attorneys entered appearances on behalf of the plaintiffs: Gary R. Buckles as local counsel on July 22, 2024 (Dkt. 12); T. Ryan Scott on July 29, 2024 (Dkt. 13); Sach D. Oliver, admitted *pro hac vice* on August 12, 2024 (Dkt. 17) and entering his appearance the next day (Dkt. 18); and Harrison A. Howle on September 16, 2024 (Dkt. 25). Robert Lambert, the state-court attorney who filed the original petition,

---

<sup>1</sup> <https://www.oked.uscourts.gov/content/jason-robertson-magistrate-judge>

never filed an entry of appearance in federal court and was permitted to withdraw on September 8, 2025 (Dkts. 137–138). On August 20, 2024, all parties consented to the jurisdiction of the United States Magistrate Judge assigned to this case. Fed. R. Civ. P. 73(b)(1). The United States Magistrate Judge exercises complete jurisdiction over this case through and including trial and the entry of a final judgment in accordance with 28 U.S.C. § 636(c)(1) and Fed. R. Civ. P. 73(a). (Dkt. 20).

**B. Substantive**

On June 20, 2025, plaintiffs' counsel (Harrison A. Howle, T. Ryan Scott, Sach D. Oliver, and Robert Lambert) filed a Sealed Response to Defendants' Motion for Summary Judgment ("Sealed Response") containing six (6) fabricated case citations, three (3) erroneous citations, three (3) quotations of nonexistent law, and five (5) misstatements of law. [Dkt. 61]. On June 30, 2025, plaintiffs' counsel filed a Motion for Partial Summary Judgment containing one (1) fabricated case citation and two (2) misstatements of law. [Dkt. 72]. On July 2, 2025, plaintiffs' counsel filed a Motion to Strike and Motion for Sanctions containing two (2) fabricated case citations. [Dkt. 78]. Plaintiffs' counsel subsequently filed six (6) Motions in Limine containing a total of four (4) fabricated case citations, two (2) quotations of nonexistent law, and one (1) misstatement of law. [Dkts. 89, 91, 92, 93, 94, 95]. On July 25, 2025, plaintiffs' counsel filed a Response to Defendants' Motion in Limine containing one (1) quotation of nonexistent law. [Dkt. 101]. And on July 27, 2025, plaintiffs' counsel filed a Reply in Support of its Motion to Strike and Motion for Sanctions containing one (1) fabricated case citation. [Dkt. 102].

Counsel for defendants filed a reply in support of summary judgment on July 29, 2025, and noted they were unable to locate multiple cases cited in plaintiffs' Sealed Response. [Dkt. 104 at 8]. On August 4, 2025, plaintiffs' counsel filed a Motion to Amend the Sealed Response and six Motions in Limine for the sole purpose of correcting "clerical and formatting errors." [Dkt. 107]. The Court thereafter engaged in a *sua sponte* review of each pleading submitted on behalf of plaintiffs during the course of this litigation and identified, *inter alia*, the following issues:

- *Williams v. Borden, Inc.*, 637 P.2d 731 (Okla. 1981) does not exist. *See* [Dkt. 61 at 14]. The Court found no cases under that citation. There is a Tenth Circuit decision under that case name, *Williams v. Borden, Inc.*, 637 F.2d 731 (10th Cir. 1980), but it does not contain the law quoted by plaintiffs' counsel.
- *Case v. Fiberboard Corp.*, 1996 OK 86, 943 P.2d 955 does not exist. *See* [Dkt. 61 at 14]. The case found at the first half of that citation is *Brashier v. Farmers Ins. Co., Inc.* 1996 OK 86, 925 P.2d 20, an action involving bad faith refusal to pay uninsured motorist benefits. The case found at the latter half of that citation is *State v. Adams*, 284 Mont. 25, 943 P.2d 955 (1997), a Montana civil rights case. There is an Oklahoma Supreme Court decision with a similar case name, *Case v. Fibreboard Corp.*, 1987 OK 79, 743 P.2d 1062, but it does not "affirm[] negligence claims for failure to implement adequate product safety practices." [*Id.*].
- *St. Louis-San Francisco Ry. Co. v. Duke*, 1959 OK 250, 363 P.2d 764 does not exist. *See* [Dkt. 61 at 17]. The case found at the first half of that citation is *Mistletoe Exp. Serv., Inc. v. Culp*, 1959 OK 250, 353 P.2d 9, a personal injury case. The Court found no cases under the latter half of that citation.
- *Brown v. Crown Equip. Co.*, 181 F. App'x 760 (10th Cir. 2006) does not exist. *See* [Dkt. 61 at 17, 20]. The case found at that citation is *Burl v. Principi*, 181 F. App'x 760 (11th Cir. 2006), an out-of-circuit employment discrimination action.
- *Austin v. Ohio Cas. Ins. Co.*, 1984 OK 41, 678 P.2d 721 does not exist. *See* [Dkt. 61 at 20]. The case found at the first half of that citation is *Thomas v. Bank of Okla., N.A.*, 1984 OK 41, 684 P.2d 553, a dispute over title to property in a revocable inter vivos trust. The Court found no cases under the latter half of that citation.

- *Lash v. Hollis*, 1978 OK 117, 571 P.2d 917 does not exist. See [Dkt. 61 at 24]. The case found at the first half of that citation is *Concannon v. Hampton*, 1978 OK 117, 584 P.2d 218, an action brought to register in Oklahoma a Missouri judgment plaintiff obtained against defendant. The case found at the latter half to that citation is *Reynolds v. Port of Portland*, 31 Or. App. 817, 571 P.2d 917, an Oregon personal injury action.
- *Creech v. Melton*, 594 P.2d 408 (Okla. 1979) does not exist. See [Dkt. 72 at 2; Dkt. 92 at 2]. The Court found no cases under that citation.
- *Two Old Hippies LLC v. Catch the Bus LLC*, 784 F. App'x 618 (10th Cir. 2019) does not exist. See [Dkt. 78 at 5]. The Court found no cases under that citation. There is a District of New Mexico decision under that case name, *Two Old Hippies, LLC v. Catch the Bus, LLC*, 274 F.R.D. 685 (D.N.M.), but it does not affirm default judgment "where discovery abuse irreversibly prejudiced the opposing party." [*Id.*].
- *F.D.I.C. v. Daily*, 973 F.Supp.2d 1116 (D. Colo. 2013) does not exist. See [Dkt. 78 at 5; Dkt. 102 at 3]. The Court found no cases under that citation. There is a Tenth Circuit decision under that case name, *F.D.I.C. v. Daily*, 973 F.2d 1525 (10th Cir. 1992), upholding the lower court's entry of default judgment in favor of FDIC for failure to comply with discovery demands and court orders.
- *White v. Deer & Co.*, No. 13-CV-437-D, 2016 WL 11750888 (W.D. Okla. Apr. 13, 2016) does not exist. See [Dkt. 91 at 2]. The Westlaw citation is an Answer Brief filed in a Florida Appeals court.
- *Morris v. Travelers Indem. Co.*, 518 F.Supp.2d 1245 (W.D. Okla. 2021) does not exist. See [Dkt. 94 at 3]. The Court found no cases under that citation. There is a Tenth Circuit decision under that case name, *Morris v. Travelers Indem. Co. of Am.*, 518 F.3d 755 (10th Cir. 2008), but it does not contain the law quoted by plaintiffs' counsel.
- *Kieffer v. Weston Land, Inc.*, No. 18-CV-794-R, 2021 WL 1099618 (W.D. Okla. Mar. 22, 2021) does not exist. See [Dkt. 94 at 3]. The Court found no cases under that citation. There is a Tenth Circuit decision under that case name, *Kieffer v. Weston Land, Inc.*, 90 F.3d 1496 (10th Cir. 1996), but it does not "exclud[e] lay opinion testimony about the cause of health problems." [*Id.*].
- *Tansey v. Dacommed Corp.*, 1994 OK 70, 890 P.2d 881 is an erroneous citation. See [Dkt. 61 at 24]. The correct citation is *Tansey v. Dacommed Corp.*, 1994 OK 146, 890 P.2d 881.
- *Wagoner v. Bennett*, 1993 OK 100, 814 P.2d 476 is an erroneous citation. See [Dkt. 61 at 24-25]. The correct citation is *Wagoner v. Bennett*, 1991 OK 70, 814 P.2d 476.

- *Thompson v. Presbyterian Hosp. Inc.*, 1982 OK 87, 652 P.2d 260 does not contain the law quoted by plaintiffs' counsel. See [Dkt. 61 at 22].
- *Howard v. Zimmer, Inc.*, 299 P.3d 463 (Okla. 2013) does not contain the law quoted by plaintiffs' counsel. See [Dkt. 61 at 24].
- *Wyeth v. Levine*, 555 U.S. 555 (2009) does not contain the law quoted by plaintiffs' counsel. See [Dkt. 89 at 2].
- *Dodson v. Bd. of Cty. Comm'rs*, 878 F.Supp.2d 1227 (D. Kan. 2012) does not hold what plaintiffs' attorneys purport. See [Dkt. 93 at 2].

After the Court's independent review revealed the scope of the inaccuracies, on August 28, 2025, the Court entered the following minute order:

“Upon further review of the documents filed by Plaintiff in this case, the hearing to receive argument on the various pending motions in this case set for September 3, 2025 at 3:00 p.m. is hereby STRICKEN. In lieu of that hearing, Plaintiff's counsel will be required to appear before this Court on SEPTEMBER 11, 2025 AT 1:30 P.M. in Courtroom 3, Room 432, U.S. Courthouse, 5th & Okmulgee, Muskogee, OK, before Magistrate Judge Jason A. Robertson, and show cause as to why sanctions should not be assessed for the filing of multiple documents with this Court which contain false or misleading information and citations. ALL COUNSEL OF RECORD REPRESENTING PLAINTIFF WILL BE REQUIRED TO APPEAR AT THIS HEARING.” (Dkt. 136).

The show-cause hearing was held on September 11, 2025, at which the Court received testimony and argument from counsel. At that hearing, Messrs. Howle and Scott appeared; Messrs. Buckles and Oliver did not. Following their nonappearance, the Court issued a Minute Order on September 11, 2025 (Dkt. 142) directing Buckles and Oliver to appear and show cause why further sanctions should not issue for failing to attend the prior hearing. That second hearing was held on October 14, 2025, at which counsel appeared and were afforded a full opportunity to be heard.

The matter was then taken under advisement and is now resolved by this written order.

### **III. ANALYSIS**

For the reasons set forth below, the Court finds that plaintiffs' counsel violated their obligation under Rule 11(b), and sanctions are warranted.

#### **A. Violations of Rule 11(b)**

Rule 11(b) is the federal lawyer's first oath in action. A standing promise that every pleading, motion, and argument submitted to a court of the United States rests on truth, law, and reason. It demands that an attorney's signature certify not creativity, but credibility: that the filing was formed after reasonable inquiry, grounded in fact, and supported by existing law or a non-frivolous argument for its extension. The rule is not aspirational; it is the minimal standard of honesty that keeps the adversarial process tethered to reality.

(b) Representations to the Court. By presenting to the court a pleading, written motion, or other paper—whether by signing, filing, submitting, or later advocating it—an attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances:

(1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation;

(2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;

(3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support

after a reasonable opportunity for further investigation or discovery; and

(4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

This obligation is absolute. It cannot be outsourced to technology or delegated to co-counsel. The attorney's signature is the personal warranty of truth that anchors the judicial process. Every one of the eleven (11) pleadings at issue was signed by Harrison A. Howle. By doing so, he certified that each filing had been reviewed and verified by human judgment. The record proves otherwise. The Court's independent review revealed twenty-eight (28) false or misleading citations: fourteen (14) fabricated cases that do not exist and fourteen (14) erroneous or misquoted authorities.

At the September 11 show-cause hearing, Mr. Howle admitted that he had used ChatGPT "to make his writing more persuasive," that the program "changed his citations," and that he did not verify them before filing. None of the eleven (11) pleadings contained the disclosure or certification required by this Court's AI Guidelines on Generative AI Disclosure and Certification.

When defense counsel notified plaintiffs' attorneys on July 29, 2025 (Dkt. 104 at 8) that several cited cases could not be located, Mr. Howle did not withdraw or correct his filings. Instead, he filed a Motion to Amend on August 4 (Dkt. 107) that described the false authorities as "clerical and formatting errors." That explanation was inaccurate. The problem was not form, it was falsity.

The Court therefore finds that Mr. Howle violated Rule 11(b)(2) and (b)(3) by presenting legal contentions not warranted by existing law and factual representations lacking evidentiary support. His conduct also contravened the duty of candor owed to the Court under Model Rule 3.3.

Responsibility under Rule 11 extends to all attorneys of record. T. Ryan Scott, who remained active in hearings and discovery; Sach D. Oliver, the supervising partner admitted pro hac vice; and Gary R. Buckles, local counsel of record, all shared an obligation to ensure that filings presented in their names were accurate. None exercised that oversight. Each failed in their role of verification, and the cumulative neglect frustrated the administration of justice.

**B. Analytical Framework for AI-Generated Filings**

Federal courts increasingly confront filings prepared with the assistance of generative artificial intelligence. While such tools can enhance efficiency, they also create a new professional hazard, synthetic authority presented as precedent. No uniform standard yet governs this issue. This Court therefore articulates the following framework, grounded in Rule 11, 28 U.S.C. § 1927, and the Court's inherent authority, to guide this Court in future cases in which AI-generated hallucinations appear in filings.

When a pleading containing fabricated citations or nonexistent law has been identified and a hearing held, this Court shall evaluate three core factors:

1. **Verification and Inquiry** — Whether counsel conducted a reasonable, human-based verification of every cited authority before filing. A reasonable inquiry

requires more than reliance on an automated tool; it demands independent confirmation through recognized primary legal sources. The signature of an attorney certifies human diligence, not mechanical output.

2. **Candor and Correction** — Whether counsel promptly disclosed the use of AI and corrected the record once inaccuracies were discovered. Candor after filing weighs heavily in mitigation; concealment or minimization aggravates the violation. The duty of candor extends beyond the moment of signature, it continues for as long as the filing remains before the Court.
3. **Accountability and Supervision** — Whether supervising or associated attorneys exercised oversight consistent with Model Rules 5.1 and 5.3 and whether firm-level safeguards existed to prevent recurrence. The inquiry extends beyond the drafter to the institutional culture that permitted unverified authority to reach the docket. A firm’s silence or absence of policy does not immunize it; it implicates it.

These factors balance culpability against mitigation and aim to deter repetition rather than destroy reputation. They also provide a path for future litigants in this Court when confronting AI-related misconduct, recognizing that the issue implicates the ethical foundations of advocacy itself.

### **C. Application of the Framework**

#### **1. Verification and Inquiry**

Mr. Howle’s admission that he relied on ChatGPT without verifying its citations demonstrates the total absence of human inquiry. Fourteen (14) fabricated

cases and fourteen (14) misquoted authorities appeared across eleven (11) pleadings: All signed by him and filed without certification. The volume and repetition of these errors show not inadvertence but systemic neglect. By contrast, Mr. Scott and Mr. Oliver did not draft the pleadings but remained counsel of record and continued to rely on them in hearings, depositions, and conferences. Their failure to examine or question the filings before advocacy reflects a secondary lapse of verification.

Mr. Buckles, as local counsel, admitted he never reviewed the pleadings and entered his appearance merely “as a favor.” His abdication eliminated the local check Rule 11 is designed to provide.

Collectively, the absence of verification at every level satisfies the first factor and represents the core breach.

## **2. Candor and Correction**

When defense counsel raised the issue on July 29, 2025, plaintiffs’ attorneys did not investigate or correct the record. Their Motion to Amend of August 4 (Dkt. 107) characterized the false citations as “clerical.” That assertion misled the Court and opposing counsel. At the show-cause hearing, Mr. Howle admitted the use of ChatGPT only after direct questioning. No earlier disclosure was made. Mr. Scott and Mr. Oliver likewise made no corrective filing despite knowing the Court was investigating. The duty of candor was breached both before and after the Court’s intervention.

### **3. Accountability and Supervision**

The Oliver Law Firm, which referred the case to Mr. Howle, maintained active involvement in discovery and strategy but had no policy governing AI use for cases referred to outside counsel and apparently conducted no review of pleadings. Its inattention enabled the misconduct.

Local counsel Gary R. Buckles provided no supervision and failed even to attend the first show-cause hearing, requiring a second order compelling his appearance. Such passivity reflects a misunderstanding of the role of local counsel, which is fiduciary, not ceremonial.

The third factor therefore weighs heavily in favor of sanctions.

#### **D. Findings under the Framework**

All three factors (verification, candor, and accountability) are met. Each demonstrates a breach of the attorney's fundamental duty of reasonable inquiry and honesty to the tribunal.

The Court does not find that Mr. Howle acted with intent to deceive. Rule 11 does not require intent; it requires responsibility. An attorney who signs eleven (11) pleadings containing fabricated authority, after using an undisclosed AI program and making no effort to verify a single citation, acts with reckless disregard for the truth. Recklessness in this context is not a lapse of diligence; it is the conscious decision to proceed in the absence of knowledge. Repetition across eleven (11) pleadings magnifies that recklessness and transforms neglect into misconduct.

The same reasoning applies, though to a lesser extent, to the supervisory and associated counsel. Their continued participation without inquiry or correction reflected indifference to accuracy once the falsity was known. Each owed the Court, and the profession, more than silence.

Accordingly, the Court concludes that plaintiffs' counsel collectively violated Rule 11(b). Their conduct, though not born of deceit, displayed a reckless disregard for the obligation to ensure that what is filed in federal court is true, verified, and worthy of the public trust. Sanctions are therefore warranted both to redress the specific harm and to deter recurrence.

#### IV. SANCTIONS

For guidance, the Court looks to other cases that have sanctioned attorneys for similar conduct. In nearly all cases, courts have imposed monetary sanctions ranging from \$1,500 to \$15,000. *See e.g., Wadsworth v. Walmart Inc.*, 348 F.R.D. 489, 499 (D. Wyo. 2025) (\$3,000 fine for the drafter of the brief with fake cases and \$1,000 for other attorneys who signed, but did not draft, the brief); *United States v. Hayes*, No. 24-CR-280, 763 F.Supp.3d 1054, 1072-73 (E.D. Cal. Jan. 17, 2025) (\$1,500 fine); *Gauthier v. Goodyear Tire & Rubber Co.*, No. 23-CV-281, 2024 WL 4882651 at \*3 (E.D. Tex. Nov. 25, 2024) (\$2,000 fine); *Mid Cent. Operating Eng'rs Health & Welfare Fund v. Hoosiervac LLC*, No. 24-CV-326, 2025 WL 574234 at \*2-3 (S.D. Ind. Feb. 21, 2025 (recommending \$15,000 fine); *Mata v. Avianca, Inc.*, 678 F.Supp.3d 443, 459 (S.D.N.Y. 2023) (\$5,000 fine for citing fake cases and then submitting AI-generated fake excerpts from the fake cases).

In some cases, courts have referred attorneys to the appropriate disciplinary body for disciplinary proceedings. *See e.g.*, Park v. Kim, 117 F.4th 610, 614 (2d Cir. 2024) (referring attorney to Second Circuit's Grievance Panel); Hayes, 763 F.Supp.3d at 1072-73 (directing Clerk of Court to serve copy of sanctions order on bar); Bevins, 2025 WL 1085695 at \*7 (directing Clerk of Court to serve copy of sanctions order on two bars); Dehghani, 2025 WL 988009 at \*6 (ordering attorney to self-report sanctions order to two bars); Hoosiervac LLC, 2025 WL 574234 at \*2-3 (referring attorney to the Southern District of Indiana's Grievance Panel).

In addition to monetary sanctions, courts have imposed more targeted sanctions given the circumstances by revoking the *pro hac vice* admission of attorneys, Wadsworth, 348 F.R.D. at 497-98, directing the Clerk of Court to serve a copy of the sanctions order on all district and magistrate judges in the district, Hayes, 763 F.Supp.3d at 1072-73, ordering attorney's fees be paid to opposing counsel for having to respond to pleadings containing fake cases, Garner v. Kadince, Inc., 2025 UT App 80, ¶ 16, 571 P.3d 812, 816, requiring the attorney to mail letters to each judge falsely identified as the author of nonexistent opinions, Gauthier, 2024 WL 4882651 at \*3, or ordering the attorney to attend CLE trainings regarding the use of AI, Dehghani, 2025 WL 988009 at \*6; Gauthier, 2024 WL 4882651 at \*3; Bunce v. Visual Tech. Innovations, Inc., No. 23-CV-1740, 2025 WL 662398 (E.D. Pa. Feb. 27, 2025).

The message from these cases is unmistakable: when attorneys abandon verification, they abandon their oath. Artificial intelligence may explain an error, but

it can never excuse one. The sanction must therefore speak not only to the lawyers before this Court, but to every lawyer tempted to trade diligence for speed. The rule is simple and enduring: truth is not negotiable, and the signature on a pleading still means something.

**A. Application of Sanctions to Individual Counsel**

When this Court first considered appropriate monetary sanctions, it looked to recent cases addressing the submission of AI-generated or fabricated authorities. In *Wadsworth v. Walmart Inc.*, 348 F.R.D. 489 (D. Wyo. 2025), fines reached \$3,000 per drafter and \$1,000 per signer. In *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023), the sanction was \$5,000 for counsel who submitted six (6) fictitious citations. Those cases involved one or two pleadings. Here, the misconduct spanned eleven (11) pleadings and twenty-eight (28) false or misleading citations: fourteen (14) fabricated, and fourteen (14) erroneous or misquoted.

Based on that scope, the Court initially contemplated fines in the range between \$10,000 and \$15,000 for the drafter and proportionate amounts for the others. However, the Court also heard testimony and observed demeanor at two hearings. Every attorney appeared (eventually), admitted the wrongdoing, accepted responsibility, and fell upon the mercy of the Court. None denied, deflected, or excused. Their contrition was genuine and complete.

Rule 11's purpose is deterrence, not destruction. The public reprimands issued in this Order, together with joint restitution of attorney's fees and the permanent

record of these findings, will deter far more effectively than excessive fines. The Court therefore exercises restraint and imposes reduced but meaningful sanctions calibrated to each attorney's degree of responsibility. These amounts (\$3,000, \$2,000, and \$1,000) stand as tangible reminders that candor is the currency of credibility before this Court.

**Harrison A. Howle — Signing and Drafting Attorney**

Mr. Howle drafted and signed every pleading at issue. By his own admission, he used ChatGPT to “make his writing more persuasive,” allowed it to alter citations, and filed the resulting briefs without verification. His actions were reckless but not deceitful.

At the September 11 hearing, he accepted full responsibility and fell upon the mercy of the Court. He has demonstrated sincere remorse. The Court credits his candor. While his conduct represented a profound failure of professional duty, it also presents a rare opportunity for public correction rather than professional ruin.

**Monetary Sanction:** \$3,000

**Public Reprimand:** Issued by this Order

**Bar Referral:** None. The Court finds no intentional deception warranting referral.

**Continued Representation:** Mr. Howle may remain as counsel of record, subject to the continuing duty to verify all future filings personally and to certify compliance with this Order.

**T. Ryan Scott — Referring Counsel and Active Participant**

Mr. Scott did not draft or sign the defective pleadings but remained counsel of record and relied upon them throughout the case. His failure to question their accuracy reflected neglect of oversight, not malice. At the hearing he admitted that

omission, accepted fault, and has since instituted firm policies requiring verification of all AI-assisted filings.

The Court initially considered a sanction of \$4,000 to \$5,000 based on his supervisory role, but his candid acknowledgment of responsibility and corrective action warrant mitigation.

**Monetary Sanction:** \$2,000

**Public Reprimand:** Issued by this Order

**Bar Referral:** None. This sanction reflects his secondary role while reaffirming that supervision is a duty, not a courtesy.

**Sach D. Oliver — Managing Partner (pro hac vice)**

As managing partner, Mr. Oliver authorized the referral to Mr. Howle and remained counsel of record. He had no policy governing AI use by associated counsel and conducted no independent review of filings submitted in his firm's name. That absence of supervision allowed unverified authorities to reach the docket.

At the October 14 hearing, Mr. Oliver accepted full accountability and pledged immediate reforms within his firm. The Court originally considered a sanction of \$2,500 to \$3,000 but, in light of his honest testimony and remedial steps, concludes that a reduced penalty will adequately deter recurrence.

**Monetary Sanction:** \$1,000

**Public Reprimand:** Issued by this Order

**Bar Referral:** None. The sanction recognizes limited direct involvement yet underscores that firm leaders remain guardians of their name and their firm's reputation on every pleading.

**Gary R. Buckles — Local Counsel of Record**

Mr. Buckles entered his appearance as local counsel on July 22, 2024 (Dkt. 12). He never met the client, never reviewed the pleadings, and did not participate in supervising out-of-district counsel. He failed to appear at the September 11 hearing, requiring a second show-cause order compelling his attendance on October 14. By his own admission, his role was purely “as a favor” to the original state-court attorney. That description underscores the systemic risk of honorary sponsorships.

Mr. Buckles’ neglect as local counsel did not create the hallucinated authorities, but it enabled them. His name on the docket gave those pleadings a presumption of legitimacy that they did not deserve. When a lawyer lends his signature, or his silence, to filings without inquiry, he converts inattention into representation and transforms friendship into liability. His conduct eroded the safeguard that local representation is meant to provide.

**Public Reprimand:** Mr. Buckles shall receive a formal public reprimand through this Order. The reprimand serves to clarify that an attorney of record, regardless of degree of involvement, is accountable for the accuracy of filings submitted under his or her name.

**Restriction on Sponsorship:** For a period of twelve (12) months, Mr. Buckles may not serve as sponsoring or local counsel for any pro hac vice attorney in the Eastern District of Oklahoma. After that period, reinstatement of sponsorship privileges will be automatic.

These sanctions, though measured, are neither symbolic nor lenient. They reflect the Court’s confidence that deterrence arises from conscience as much as from cost. The combination of public reprimands, individual fines, and full restitution of

attorney's fees restores the balance Rule 11 demands: truth verified, accountability imposed, and integrity reaffirmed.

All counsel are admonished that the trust restored today must be maintained tomorrow. The record of this Order will stand as both warning and witness that verification is not optional, and that mercy in this Court is always tethered to responsibility.

### **B. Remedial Correction of the Record**

The purpose of sanctions under Rule 11 is not only to deter future misconduct but also to restore the integrity of the record already before the Court. Pleadings that rely upon fabricated or erroneous authorities cannot remain on the docket. They misstate the law, distort the issues, and leave the Court to build upon a foundation that no longer exists.

Accordingly, all filings identified in this Order as containing fabricated or inaccurate citations are hereby STRICKEN from the record. This includes the following docket entries: 61, 72, 78, 89, 91, 92, 93, 94, 95, 101 and 102.

Within sixty (60) days of the date of this Order, Plaintiffs shall file verified amended pleadings that show as follows:

1. drafted and reviewed by human counsel without the use of generative artificial intelligence tools to produce or alter text or citations, except as expressly permitted by this Court's AI Guidelines on Artificial Intelligence Disclosure and Certification;

2. contain only accurate and verifiable authorities; and,
3. are accompanied by a signed Certification of Verification confirming that counsel personally reviewed each cited case, statute, or exhibit for accuracy.

The Certification shall state:

“I certify that I personally reviewed each citation and authority referenced in this pleading and that, to the best of my knowledge and belief, all citations are genuine and accurately reflect the law as of the date of filing. This filing complies with the requirements of the Court’s AI Guidelines on Artificial Intelligence Disclosure and Certification.”

Failure to file verified pleadings within the sixty-day period will result in dismissal of those claims without further notice.

This directive is restorative. The record must reflect truth before the Court may apply law. The Federal Rules presuppose a foundation of accuracy, and where that foundation has been compromised, the only remedy is reconstruction. The Court therefore wipes the slate clean, in the service of veracity. Having restored the integrity of the record, the Court now turns to the question of cost, specifically, the burden unjustly borne by opposing counsel in responding to pleadings that no longer exist.

**C. Award of Attorney’s Fees and Costs**

Under Rule 11(c)(4), a sanction “may include ... an order directing payment to the movant of part or all of the reasonable attorney’s fees and other expenses directly resulting from the violation.” The Court finds that the defendants’ counsel incurred

substantial expense responding to the fabricated filings and addressing the procedural disruption that followed.

The Affidavit of Theresa N. Hill, lead counsel for defendants Cosway Company, Inc. and Product Innovations Research, LLC, establishes that her firm, Rhodes, Hieronymus, Jones, Tucker & Gable, PLLC, expended \$23,423.50 in attorney fees and \$72.40 in costs, for a total of \$23,495.90, in connection with these pleadings and the resulting hearings. The Court finds these fees and expenses reasonable and directly caused by the violations identified in this Order.

Accordingly, pursuant to Rule 11(c)(4), the Court orders joint and several reimbursement of these amounts by the Howle Law Firm and the Oliver Law Firm, in equal shares. Each firm shall remit \$11,747.95 to defense counsel within thirty (30) days of this Order. This obligation is separate from the individual monetary sanctions imposed above and shall not be borne by local counsel Gary R. Buckles.

The Court directs defense counsel to file a short notice of compliance once payment is received.

The purpose of these sanctions is not punitive but restorative: to restore the meaning of local appearance and to reinforce the Court's expectation that every lawyer of record, regardless of title, stands as both advocate and guarantor of integrity. The Court expects compliance not because it demands perfection, but because the justice system cannot function without verification.

## V. CONCLUSION

The Court has imposed sanctions to restore, not to ruin. The aim of this ruling is not punishment for its own sake, but the reaffirmation of professional honor.

All counsel have appeared, accepted responsibility, and sought mercy. The Court has answered with proportion, acknowledging their contrition while ensuring accountability endures. The combination of public reprimand, restitution, and monetary penalty satisfies the Rule 11 standard of deterrence and reaffirms that the practice of law is an act of trust.

The lesson is neither new nor novel. The practice of law has never been about convenience; it has always demanded courage. The quiet, disciplined courage to stand for what is right when compromise would be easier. Marcus Aurelius wrote, "If it is not right, do not do it; if it is not true, do not say it." *Meditations* bk. 12, § 17 (Gregory Hays trans., Modern Library ed. 2002). That simple maxim captures the heart of advocacy: the moral courage to write, to argue, and to sign only what truth can defend.

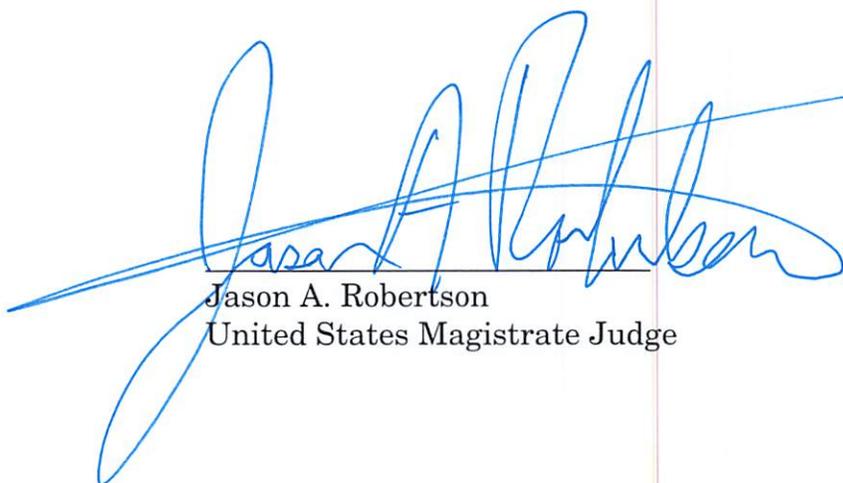
It takes courage to put a word, a sentence, a phrase to paper in defense of another. It takes courage to sign one's name beneath arguments that carry the weight of justice. Machines can assemble words, but they cannot believe in them. They can process information, but they cannot possess conviction.

The Court does not fear progress. It fears abdication. When lawyers trade reflection for automation, they surrender the very quality that makes their words

worthy of belief. The oath of candor is not a relic; it is the living covenant between the advocate and the tribunal. It binds judgment to integrity and intellect to honor.

Generative tools may assist, but they can never replace the moral nerve that transforms thought into advocacy. Before this Court, artificial intelligence is optional. Actual intelligence is mandatory.

IT IS SO ORDERED this 22<sup>nd</sup> day of October 2025.

A handwritten signature in blue ink, appearing to read "Jason A. Robertson", is written over a horizontal line. The signature is stylized and cursive.

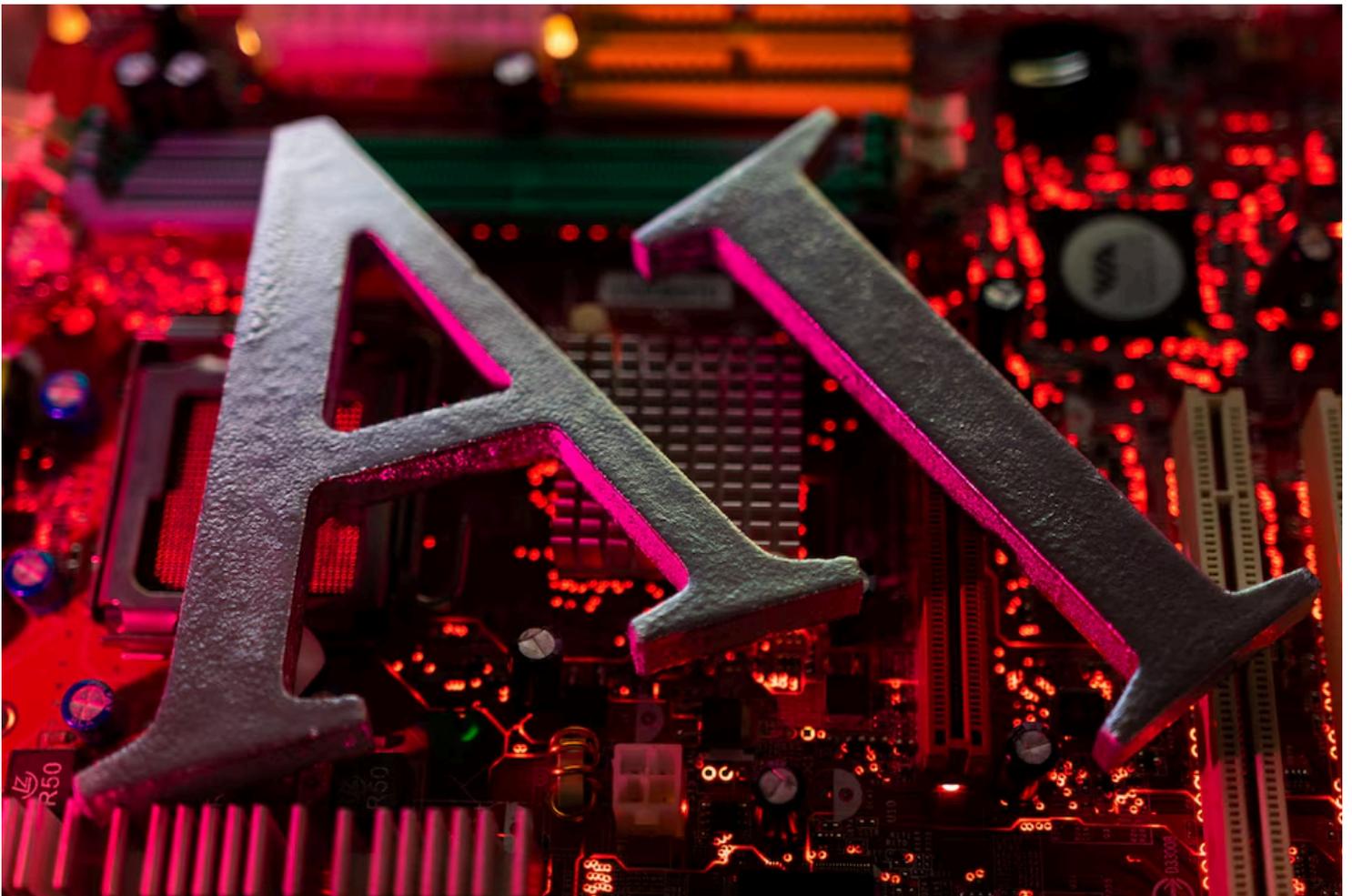
Jason A. Robertson  
United States Magistrate Judge

Learn more about [LSEG](#)

## New York court system sets rules for AI use by judges, staff

By Sara Merken

October 10, 2025 3:39 PM CDT · Updated October 10, 2025



AI (Artificial Intelligence) letters are placed on computer motherboard in this illustration taken, June 23, 2023. REUTERS/Dado Ruvic/Illustration [Purchase Licensing Rights](#)

Oct 10 (Reuters) - The New York state court system on Friday set out a new policy on the use of artificial intelligence by judges and other court staff, joining at least four other U.S. states that have adopted similar rules in the past year.

The [interim policy](#), which applies to all judges, justices and nonjudicial employees in the New York Unified Court System, limits the use of generative AI to approved products and mandates AI training.

The Week in Breakingviews newsletter offers insights and ideas from Reuters' global financial commentary team. Sign up [here](#).

New York's policy prohibits judges and staff from inputting confidential or privileged information, or documents that have been submitted in court, into a generative AI program that doesn't operate on a private model. Private models, as defined by the policy, operate under the control of the court system and do not share data with public tools.

The court did not immediately respond to a request for comment about how the new policy would be monitored.

It is "critical to ensure that material that reflects harmful bias, stereotypes, or prejudice" does not appear in work product, according to the policy. Judges and staff are responsible for their work, and AI technology must be used in a manner consistent with their ethical obligations, the policy states.

"While AI can enhance productivity, it must be utilized with great care," Chief Administrative Judge Joseph Zayas said in a statement. "It is not designed to replace human judgment, discretion, or decision-making."

States including [California](#), [Delaware](#), [Illinois](#) and Arizona have adopted AI rules or policies, while other states are assessing the use of generative AI within their courts.

Lawyers across the country have increasingly been hit with [fines and other sanctions](#) from judges for apparent misuse of AI, as fictitious case citations and other errors continue to show up in legal filings. Professional conduct rules don't bar lawyers from using AI, but attorneys can be disciplined for failing to vet court submissions.

Judges are also facing scrutiny. U.S. Senate Judiciary Committee Chairman Chuck Grassley on Monday [asked two federal judges](#) to answer questions about whether AI was used to prepare recent orders that contained "substantive errors."

Reporting by Sara Merken

Our Standards: [The Thomson Reuters Trust Principles](#).

Suggested Topics:

Government

Judiciary

Legal Innovation

Data Privacy

## Purchase Licensing Rights



**Sara Merken**  
Thomson Reuters

Sara Merken reports on the business of law, including legal innovation and law firms in New York and



my news



## Read Next / Editor's Picks

Government

### US review of Alex Pretti killing does not mention him brandishing firearm

18 mins ago



Government

### Judge blocks Virginia lawmakers' bid for pro-Democratic voting map

8 hours ago



Government

### Texas governor halts new H-1B visa petitions by state agencies, public universities

January 27, 2026



Government

### US judge threatens ICE chief with contempt, orders court appearance

January 27, 2026



# JUDGING AI:

## HOW U.S. JUDGES CAN HARNESS GENERATIVE AI WITHOUT COMPROMISING JUSTICE

BY XAVIER RODRIGUEZ



## IN A VOTING-RIGHTS TRIAL WITH THOUSANDS OF PAGES OF EVIDENCE, GENERATIVE AI TOOLS OFFERED A GLIMPSE OF HOW TECHNOLOGY MIGHT EASE THE JUDICIARY'S HEAVIEST BURDENS.

**E**-discovery tools that harness the power of artificial intelligence (AI) assist attorneys somewhat regularly.<sup>1</sup> But my recent experience presiding over a bench trial in *La Union Del Pueblo Entero v. Abbott* showed me that generative AI (GenAI) can help judges in several crucial ways that go far beyond discovery.

*La Union Del Pueblo Entero* was a consolidated action brought by advocacy groups, voters, and an election official challenging two dozen provisions of an omnibus election law enacted in Texas in 2021, known as S.B. 1, under various federal civil rights statutes and the U.S. Constitution. In all, there were approximately 80 witnesses (both live and by deposition testimony), nearly 1,000 exhibits, and more than 5,000 pages of trial transcripts.

This case provided an opportunity to evaluate how GenAI might help a judge in a complex and document-intensive case. This article explores how GenAI can help locate documents and summarize witness testimony, whether GenAI tools are currently capable of completing a rough draft of a judicial opinion, and how GenAI can review party submissions.

### LOCATING DOCUMENTS: SAVING TREES AND CUTTING TIME

The first challenge facing my chambers was simply how to locate the exhibits and relevant portions of testimony as we began researching and drafting findings of fact and conclusions of law (FFCL).

While the federal court's electronic case filing system (ECF) permits full-

text searches of docket filings, its functionality is limited. First, it relies on keyword search, which tends to be both over- and under-inclusive. Second, many documents filed on ECF have not been run through optical character recognition (OCR) software, rendering them unsearchable. Third, ECF searches do not permit judges to limit their queries to specific documents on the docket or to search documents that have been submitted to the court but not yet filed. Thus, a search for a party name, for example, would likely turn up every document filed in the case — not a particularly helpful exercise.

I teach an e-discovery law school course, and over the past 10 years, many vendors have graciously provided my students with access to their review platforms. I give my students requests for production and require them to use the relevant platform to provide the number of “hits” they believe are responsive. Given the difficulty my chambers would have in locating relevant exhibits, I immediately thought of turning to an e-discovery provider to ingest, index, and grant me access to a review platform that I could use to locate documents (or portions of documents) needed during the drafting process.

Merlin,<sup>2</sup> an e-discovery vendor, agreed to help me, and — after the court's IT department vetted the company for cybersecurity concerns — we uploaded about a thousand documents representing all the trial testimony, admitted exhibits, the parties' briefings and proposed FFCL, and my earlier

orders in the case to a secure site created specifically for our project.

Merlin's OCR and integrated keyword and algorithmic search capabilities (Search 2.0) allowed my chambers to quickly locate key documents and testimony without crafting complicated searches. Like many e-discovery tools I have used, Merlin permits users to tag documents by relevant fields.

Given the evolution of GenAI in recent years, I was interested in testing out other uses for these tools in my chambers, including tasks — such as summarizing evidence and drafting factual findings — and reviewing our work product.

One note, however: Judges and attorneys considering using these GenAI tools should be cautious in uploading any data that is confidential, privileged, or otherwise contains sensitive data (e.g., financial or health information). In particular, users should ensure that the provider's large language model (LLM) does not use any nonpublic data to train its system and that the provider has adequate cybersecurity measures in place.<sup>3</sup>

### SUMMARIZING TEXT: GENERATING OVERVIEWS OF WITNESS TESTIMONY

GenAI has a unique ability to summarize text data. Although GenAI summarization can struggle with some types of information, judges and lawyers may find GenAI to be useful for analyzing trial and deposition testimony. Deposition and transcript summaries are a standard way to extract, condense, and organize information from ►

*Running a simple prompt requesting a summary of the process for curbside voting in Texas, Merlin produced a comprehensive response within seconds, pulling from both deposition and trial testimony and across multiple witnesses.*

testimony that may be spread over the course of hundreds — or thousands — of pages and multiple days of examination. While useful, they can be time-consuming (and expensive) to create and, depending on how they are structured, can produce inflexible results.

To conduct this task manually, the judge or lead counsel must determine how the transcript will be summarized (e.g., chronologically, by witness, or by topic). Then, a more junior attorney or legal assistant must locate the portions of the transcript they intend to summarize, typically by running keyword searches against transcripts. Finally, of course, they read and summarize the portions of the testimony they identified through their keyword searches, including pin cites to the pages and lines of the transcript along the way.

Even high-quality manual summaries can be cumbersome to use during the writing process, because, like the underlying transcripts themselves, they are static. For example, an attorney may find it difficult to quickly identify testimony about a certain topic if the summaries have been organized by date or witness. At the same time, because the purpose of the summaries is typically to help attorneys locate relevant testimony in the transcript — to be quoted or cited in briefing — summarization itself often represents the first step in a tedious, iterative process that takes attorneys from transcripts to summaries and back again (and again).

GenAI systems deploying retrieval-augmented generation (RAG), including Merlin's, are particularly well-suited to summarizing transcript testimony because they mirror the manual process, albeit with much greater speed, power, and agility. RAG reduces

hallucination by deploying an LLM's language capabilities to answer questions in the context of a constrained data set through a two-step process: "(1) retrieval and (2) generation."<sup>4</sup>

When a user submits a question to a RAG system, it first searches a set of documents defined by the user to find the most relevant passages. In the second step, generation, the system provides the relevant documents and original query to an LLM, which uses both inputs to generate an "open-book" answer.<sup>5</sup>

As an experiment, I compared my staff's summarization skills (and speed) against Merlin's. I asked my law clerks and interns familiar with the case to summarize portions of the trial testimony and keep track of the time it took them to review the testimony and prepare a summary (with relevant citations to the record).

Many resources report that it takes an experienced attorney or paralegal one hour to summarize about 25 pages of deposition testimony. Suffice it to say, it took my law clerks and interns much longer to summarize the testimony in my case (which I attribute to their desire to be exacting in their work).

Running a simple prompt requesting a summary of the process for curbside voting in Texas, Merlin produced a comprehensive response within seconds, pulling from both deposition and trial testimony and across multiple witnesses. (In fairness to my intern, I asked him to produce a summary of the process based on testimony from a single witness on a single day of trial.) The two responses follow below.<sup>6</sup>

**Intern's response:** The curbside voting process begins with the press of a button, which calls an

election worker to the vehicle. Tr. at 704:15–17. Often, a brief wait ensues before an election worker is available. Tr. at 705:4. The election worker then takes the voter's identification (and that of any assistor) and authenticates the voter's registration status before disbursing the ballot materials. Tr. at 704:4–8. A private assistor must sign the Oath of Assistance under S.B. 1. Tr. at 709: 14–18. As soon as a voting machine becomes available, the election worker must wheel it out to the vehicle and position it in front of the voter, so that the voter (and, if applicable, a private assistor) can read the options on the ballot and make his selections on the machine. Tr. at 705:21–24, 706:7–13, 706:21–24, 707:6–7. The entire process may take upwards of 45 minutes. Tr. at 707:24.

**Merlin's response:** Curbside voting in Texas is a process designed for voters who are physically unable to enter the polling place without assistance or at the risk of injuring their health. An election officer delivers a ballot to the voter at the entrance or curb of the polling place if curbside voting is requested. Tr. at 827:4–12. Curbside voting is available at every polling location across Texas. Tr. at 1152:8–13.

The process involves a voter signaling for assistance, after which an election worker verifies their ID, brings the equipment out, the voter marks their ballot, and the worker takes the ballot inside to scan it. Tr. at 1152:19–1153:3. In some cases, when a voter arrives for curbside voting and there are

no workers outside, they can call a number that rings the [election] judge’s cell phone to request voting assistance. Scarpello Dep. at 276:14–19. The [election] judge then sends a worker with an electronic poll book to the voter, who signs it, and the worker retrieves the voting machine and brings it out for the voter to cast their ballot. Scarpello Dep. at 276:14–19.

All election workers in Harris County are trained on curbside voting, indicating that it is a standard practice. Tr. at 1152:14–16. The security of curbside voting is considered to be on par with that of in-person voting inside the polling place, as the procedure is the same whether conducted inside or outside the building. Scarpello Dep. at 276:20–25.

It is important to note that curbside voting is distinct from drive-through voting, which was offered in Harris County during the November 2020 election. Drive-through voting allowed voters to pull up in their vehicle, mark their ballot at the machine outside, and then deposit their ballot into the scanner themselves, without the ballot ever leaving the voter’s sight. Tr. at 1153:4–1154:17. However, drive-through voting . . . was offered [to all Harris County voters in November 2020] to provide more accessibility and opportunities for people to vote. Tr. at 1154:18–1155:5. Curbside voting, on the other hand, is specifically for eligible voters who meet certain criteria and is a method that has been offered by all counties across Texas. Tr. at 1236:22–1237:14, 1237:21–25.

Of course, the fact that a GenAI tool creates a summary at a fraction of the

time (and likely cost) of human-generated summaries must be balanced against the accuracy and usefulness of the GenAI summaries, which humans must ultimately evaluate. In my case, I used the summary as a launching point to locate the relevant evidence. The intern’s summary was a bit more focused, while Merlin’s response was slightly more general. Had the goal been to incorporate the summary wholesale into a draft opinion, the intern’s work would have proved more useful.

Like other programs I have reviewed, Merlin enables users to evaluate the accuracy of its summaries by providing citations to supporting evidence with links to the original source documents. Thus, in instances where the summary seemed a bit shallow, a mere click on the record link allowed my chambers to quickly find additional details and context. Merlin also allows users to download (or copy and paste) both responses to prompts and the AI-generated summaries of the underlying documents. (See this article at [judicature.duke.edu](http://judicature.duke.edu) for visuals of these summaries.)

#### DRAFTING: FIRST PASSES AT ORDERS

After test-driving GenAI’s summarization capabilities, I was curious about its ability to analyze and make judgments about the information stored in the review platform. I asked Merlin to draft findings of fact<sup>7</sup> on one of the causes of action in the election case.

First, I did not (and will not currently) use any GenAI product to draft orders or FFCLs ultimately filed in a case. I ran the prompts in Merlin discussed below only *after* my chambers had published the FFCLs on the plaintiffs’ challenges under the First Amendment and Section 208 of the Voting Rights Act in the traditional manner.<sup>8</sup>

Second, I do not advocate that GenAI be used as a substitute for judicial decision-making, for many reasons. A GenAI response might be partially or even completely inaccurate. A judge may unintentionally become “anchored” to the GenAI’s response — sometimes referred to as automation bias, a phenomenon in which humans trust GenAI responses as valid without validating the results. Similarly, a judge might be influenced by confirmation bias, where a human accepts the GenAI results because they align with the beliefs and opinions already held.

That said, I do not doubt that GenAI tools can be used to *assist* judicial officers in performing their work more efficiently. A GenAI tool could also be used after a draft of an order or opinion is completed to verify or question the draft’s accuracy, and confirmation bias can occur without the use of an AI tool.

#### *Prompt 1: Findings of Fact on a Single Theory of Liability*

In my first test, with assistance from the Merlin team, I prepared a prompt seeking findings of fact and conclusions of law on a single theory of liability: that a restriction on certain “compensated” canvassing activities “in the presence of” mail-in ballots (the canvassing restriction) is overbroad and chills free speech in violation of the First Amendment. I requested a legal opinion that would identify the parties, outline the procedural history of the case, assess the impact of the canvassing restriction, discuss the parties’ standing, and evaluate the merits of their challenge.

Merlin used an AI chatbot app called Claude 3.5 Sonnet in two capacities: first, to produce 1,685 summaries (reflecting the entire universe of documents uploaded to the platform) and ▶

*I had asked Merlin to draw inferences and connections based on legal reasoning not made explicit anywhere in the trial transcript or evidentiary record. Accordingly, iteration – refining and optimizing prompts – was necessary.*

then to produce a 12-page narrative response to my prompt based on the summaries.<sup>9</sup> The results of the first test quickly revealed the first insight of my experiment: GenAI is not yet ready to replace judges (phew!). As the saying “garbage in, garbage out” suggests, its outputs are only as good as its inputs, both in the quality of information sources being mined and the prompts submitted to the platform.

To begin, the results were overbroad. For example, although my prompt requested information about the canvassing restriction, the answer discussed several other provisions of S.B. 1 being challenged in the litigation, as well as parties who were not challenging the canvassing restriction, including some who had been dismissed from the case entirely.

Of the dozen pages that Claude 3.5 Sonnet produced, only two or three were relevant.

To the extent they were relevant, the analysis included within them was often quite superficial. For example, in its discussion of standing, the answer stated, “Many organizational plaintiffs have demonstrated standing by showing (a) Diversion of resources to counteract S.B. 1’s effects, (b) Chilling effect on their activities, (c) Concrete changes in operations, [or] (d) Harm to their members’ voting rights.” These generic descriptions of the bases for organizational standing did not speak to the question at hand – which, if any, of the plaintiffs had standing to challenge *the canvassing restriction* specifically. Even more targeted responses were too vague to provide a clear basis for standing. A statement that “Mi Familia Vota express[ed] concerns about potential accusations of vote harvesting during

legitimate voter outreach activities” does not identify the nature of those activities or whether the organization has decided to modify or cease its outreach activities.

Thus, to effectively use GenAI as a tool in judicial opinion writing, judges and their staffs will still need to exercise *judgment*:

- Judges must still be familiar with the factual and legal disputes at the hearts of their cases to develop prompts that yield relevant and accurate results.
- Judges also need to consider the limitations of the specific tool being used and the nature (and scope) of the evidentiary record.
- Finally, as discussed above, judges must evaluate the relevance, accuracy, and limitations of the results.

Based on the initial results, I knew I had to make some changes to my prompts because of the case, the underlying documents, and Merlin’s capabilities.

For example, I realized that I should limit my request to factual findings rather than asking Merlin to prepare legal conclusions, for a few reasons.

First, because Merlin is not connected to a legal database and is instead drawn from a closed universe of documents, it was not designed to produce legal analyses.

In this case, the parties disagreed about the legal standard for evaluating the First Amendment challenge. The plaintiffs argued that strict scrutiny should apply, while the defendants proposed a lower standard under the *Anderson-Burdick* line of cases.

Although Merlin and I ultimately both applied the same standard – strict scrutiny – I suspect that Merlin defaulted to the plaintiffs’ proposed

standard simply because they filed more briefs than the defendants. Differences in quantity may be relevant for the purpose of analyzing propensity and/or the weight of the evidence, but the quantity of briefing in support of a given legal standard obviously does not affect which standard judges should apply (and may not even reflect the weight of authority).<sup>10</sup> Moreover, while the trial record is static following the close of evidence, legal standards can change during the course of litigation – and did in this particular case. In any event, for this project, I was interested in testing GenAI’s ability to analyze and synthesize evidence to make factual findings – its ability to act as a jury, not a judge – because making fact findings often represents the most time-consuming and resource-intensive part of a judge’s work following a bench trial.

Second, given certain limitations in the evidentiary record, it also became clear that, to ensure relevant results, the prompt should center on the factual findings necessary to support the plaintiffs’ specific legal theories rather than ask about the legal theories themselves. In other words, I had to bake some judgments and assumptions about the facts and claims into my prompt.

For example, while my initial prompt asked Merlin about First Amendment challenges to the canvassing restriction, the response addressed facts bearing on all kinds of claims asserted by the plaintiffs (e.g., racial disparities) and discussed other portions of the law (e.g., an ID-number matching requirement for mail voting). I expect that these responses appeared because, at trial, many witnesses for civil rights groups who testified about the canvassing restriction’s chilling effect on their speech were also asked about its effects

on specific groups of voters and about the impact of other provisions of the election code at issue in the litigation.

With good reason, attorneys did not constantly reference the applicable theory of liability in each of their questions at trial. Not only would it have been an unbearably awkward form of questioning, but many questions were also intended to elicit responses relevant to multiple claims. And, in addition to potentially confusing lay witnesses, asking them to describe how the canvassing restriction impaired their First Amendment rights would have required them to draw improper legal conclusions. Instead, witnesses were asked questions about the effect that the canvassing restriction had on their interactions with voters (i.e., *facts* relevant to their overarching legal theories). It is unsurprising, then, that the results of my initial prompt were both under- and over-inclusive to a certain degree — I had asked Merlin to draw inferences and connections based on legal reasoning not made explicit anywhere in the trial transcript or evidentiary record. Accordingly, iteration — refining and optimizing prompts — was necessary.

### **Prompt 2: Findings of Fact Only, With Specific Instructions**

#### **My revised prompt:**

Assume you are a United States district judge presiding over a bench trial concerning First Amendment free speech and overbreadth and Fourteenth Amendment due process challenges to the “vote harvesting ban” under Texas Election Code section 276.015, enacted as Section 7.04 of the Texas Election Protection and Integrity Act of 2021 (commonly known as “S.B. 1”).

Please prepare detailed findings of fact concerning plaintiff organiza-

tions’ First Amendment free speech and overbreadth and Fourteenth Amendment void-for-vagueness due process challenges under 42 U.S.C. Section 1983 with Federal Rule of Civil Procedure 52, based on a comprehensive review of the trial testimony, exhibits, and briefs submitted by all parties. Your findings should address the following key areas:

#### **1. Challenged Provisions**

Describe Section 7.04 and define it as the “Canvassing Restriction.” In your response, please refer to Section 7.04 of S.B. 1 as either Section 7.04 or the “Canvassing Restriction.”

#### **2. Procedural History**

Outline the chronology of the First Amendment and challenges to Section 7.04 from initial filing to the conclusion of the bench trial. Include key motions, rulings, and any significant pretrial events.

#### **3. Parties**

Provide the following information about the parties:

- **Plaintiffs:** Identify and describe the following plaintiffs in separate paragraphs with bold headings: League of United Latin American Citizens – Texas (LULAC), Texas American Federation of Teachers (AFT), Texas Alliance for Retired Americans (TARA), La Union Del Pueblo Entero (LUPE), and Mexican American Bar Association of Texas (MABA).
- **Defendants:** Identify and describe the following defendants: the Texas attorney general, the Texas secretary of state, and the district attorneys of Travis County, Dallas County, Hidalgo County, and the 34th Judicial District, including their respective authority under

Texas law to enforce, investigate, and prosecute crimes under the Texas Election Code and evidence of their willingness to do so, with special attention to “vote harvesting” crimes.

#### **4. Difficulties and Confusion in Interpreting Section 7.04**

Give examples of the difficulties and confusion trial witnesses (including voters, organizational representatives, canvassers, assistants, election officials, and state officials) have experienced in interpreting Section 7.04, including:

- The meaning of “physical presence” and “compensation,” and
- Whether the Canvassing Restriction prevented canvassers from providing mail-ballot voting assistance.

Make sure to cite specific testimony by individuals wherever possible regarding these issues, providing as many citations to trial testimony as possible.

#### **5. Section 7.04’s Impact on Plaintiffs’ Free Speech and In-Person Voter Outreach Efforts**

Provide factual conclusions showing how Section 7.04 has limited the plaintiff organizations’ free speech and in-person voter outreach efforts, including canvassing, hosting election events, and providing voter assistance.

Make sure to cite specific testimony by individuals wherever possible regarding these issues, providing as many citations to trial testimony as possible.

In response, Merlin produced a 10-page written response — with impressive results. ►

## *While concerns about cutting corners arise out of legitimate problems – including systemic resource disparities and individual bad apples – much of the ire and fear directed at the use of AI is, in my view, misplaced.*

While the response to my first prompt produced two vague descriptions of the “chilling effect” of the canvassing restriction (“Organizations like Mi Familia Vota express concerns about potential accusations of vote harvesting during legitimate voter outreach activities.”), the second report provided specific and accurate examples of voter outreach activities that had been impaired:

- OCA-Greater Houston (Organization of Chinese Americans) canceled candidate forums, limited involvement in co-sponsored events, and shifted to virtual formats for meet-and-greets.
- Organizations have reported difficulty in recruiting volunteers willing to provide voter assistance due to concerns about criminal penalties.
- FIEL (Familias Inmigrantes y Estudiantes en la Lucha) discontinued its “caravan to the polls” activities due to concerns about potential legal consequences under S.B. 1.
- LULAC has scaled back or stopped completely its voter assistance programs in some areas due to fear of prosecution.
- Texas AFT has significantly reduced its canvassing efforts, shifting to alternative outreach methods like texting, letter campaigns, and phone calls.
- TARA stopped accepting or setting up tabling invitations during the period when mail ballots are out.
- OCA-Greater Houston has stopped providing voter assistance, including language assistance to Chinese-speaking voters, due to concerns about S.B. 1.

Unlike the response to my first prompt, the second report also described wit-

ness testimony explaining the basis for the canvassing restriction’s chilling effect on political speech — its broad and vague terminology:

- Keith Ingram from the Texas Secretary of State’s Office stated that both the voter and the harvester must be looking at the ballot together for an interaction to be considered “in-person,” but could not provide a specific distance for what constitutes “in-person interaction.”
- Grace Chimene from the League of Women Voters expressed concern that even small gestures like offering tea, coffee, or parking assistance could be considered compensation.
- Deborah Chen from OCA-Greater Houston expressed confusion about whether providing water bottles or T-shirts to volunteers could be considered compensation.
- Jonathan White, a state official, acknowledged that further research would be needed to determine if things like gift bags or meals count as compensation.

### **REVIEWING JUDICIAL DRAFTS AND PARTY SUBMISSIONS**

While conducting tests with Merlin, I had an opportunity to try another GenAI tool, Clearbrief. Like Merlin, Clearbrief allows users to upload sources to a secure site devoted to a specific project.

Employing OCR and search technology as Merlin does, Clearbrief enables users to quickly find information in the underlying documents. While Merlin functions as a separate site, Clearbrief operates through a Microsoft Word add-in. This feature lets users extract text from the record and paste it directly into a draft Word document (automatically including a record citation).

Clearbrief can generate timelines, topic tables, and deposition summaries based on uploaded documents, though it does not produce prompt-based summaries of the underlying information. Clearbrief also has access to legal resources available on LexisNexis and in the public domain, which allow it to score how well sentences in a brief or opinion are supported by the cited legal (or factual) authority.

Clearbrief’s combined capabilities have allowed my chambers to prepare timelines of case events and verify the accuracy of briefs and record citations, which can be helpful during status conferences and hearings. They have also helped my chambers review and cite-check drafts of my opinions before they are published.

### **THE LAST WORD**

The voting rights case presented a unique opportunity to assess the current state of GenAI proficiency at various tasks and to experiment with ways to improve its performance. Rather than treating all platforms as one-size-fits-all, courts considering adding GenAI to their toolboxes should determine whether an à la carte approach would better serve judges’ needs in some cases.

Merlin’s summarization capabilities may be more helpful for large-scale, complex, fact-intensive cases — as it was in this one — since each project requires creating a new and separate secure site. Yet Clearbrief’s technology may be more helpful for some of the everyday work of the judiciary, such as preparing for status conferences and hearings, reviewing briefs, and cite-checking opinions.

A few widely publicized misuses of AI in the legal profession have caused

moral panic in some circles (including the judiciary), rendering “AI” a four-letter word. While concerns about cutting corners arise out of legitimate problems — including systemic resource disparities and individual bad apples — much of the ire and fear directed at the use of AI is, in my view, misplaced. As I like to point out, attorneys have been hallucinating cases since long before AI.

To be sure, there are bad and lazy (and overworked) attorneys in the world. But refusing to deploy GenAI technology in the judiciary will not stop those attorneys from citing cases that do not exist or supplying faithless summaries of a factual record. It will only ensure that the judicial task of detecting such misdeeds is unnecessarily cumbersome.

There are also bad and lazy (and overworked) judges. Refusing to deploy GenAI technology in the judiciary will not protect the litigants who come before them from the deficiencies in their chambers. While some have expressed concern that permitting judges and clerks with access to AI features of legal databases will use it as a substitute for legal research, the same judges and clerks could easily (without AI) substitute the prevailing parties’ briefing for legal research. In other words, uncritically copying and pasting is not a sin exclusive to AI.

Moreover, to the extent that individual judges are willing to uncritically accept GenAI results, that decision (and accompanying risks to their reputations and appellate reversal rates) are better left to judges themselves rather than court administrators. Given judges’ broad authority to make significant and far-reaching — sometimes even life-or-death — decisions in the U.S. legal tradition, there is some irony in the suggestion that they cannot be trusted

to make prudent decisions about whether and how to use a technological tool to support their work.

As my experiments demonstrate, the effective use of GenAI to support judicial work will still require attention to detail and good judgment, both in crafting prompts and using the results. But GenAI can be a helpful tool for improving judicial efficiency, cutting out much of the tedious legwork of locating, collecting, and describing facts in the record and arguments by the parties.

GenAI tools can be readily used by judges in preparation for initial scheduling conferences by quickly generating timelines and summaries that allow for more meaningful conferences with litigants about, e.g., the appropriate scope of discovery, the possibility of alternative dispute resolution, and even the viability of their respective legal theories. GenAI can also be used to help prepare judges for hearings on motions to dismiss or motions for summary judgment. The state of GenAI tools is such that, at the time of our testing, they could not create judicial opinions or substantive orders, but with responsible use, they can assist judges in more efficient adjudication of the cases before them. The GenAI landscape is rapidly shifting, of course, and as existing platforms continue to evolve and new products emerge, they may be able to generate something closer to a final product.<sup>11</sup> Still, there’s no substitute for good judgment.



**XAVIER RODRIGUEZ** is a U.S. district judge for the Western District of Texas and a 2023 graduate of Duke Law School's Master of Judicial Studies program.

<sup>1</sup> My thanks to my career law clerk, Caroline Bell, for her assistance as we explored AI tools for chambers use, and for her contributions to this article. My thanks also to Allison H. Goddard, U.S. magistrate judge for the Southern District of California, and Maura Grossman, research professor at the University of Waterloo, for their review of this article and their suggestions.

<sup>2</sup> For more information on these products, see generally MERLIN SEARCH TECHNOLOGIES (2024), <https://www.merlin.tech/>; CLEARBRIEF (2025), <https://clearbrief.com/>. I do not endorse any e-discovery or AI product. References to any product are solely for illustrative purposes as to what certain products can do and what limitations may arise.

<sup>3</sup> The American Institute of Certified Public Accountants has defined criteria for managing customer data based on “five Trust Services Criteria . . . security, availability, processing integrity, confidentiality, and privacy.” Danielle Marie Hall, *What Is Candle AI?*, ABA L. PRAC. MAG. (July 3, 2025), <https://duke.is/y/m8z3>. Many GenAI commercial providers contractually agree that they will not use prompt information for training. All users should review terms of service before using a product.

<sup>4</sup> See Varun Magesh et al., *Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools*, 22 J. OF EMPIRICAL LEGAL STUD. 216, 219 (2025).

<sup>5</sup> *Id.*

<sup>6</sup> These summaries have been lightly edited for clarity and consistency.

<sup>7</sup> Merlin is not able to generate conclusions of law since it is not trained on U.S. legal authorities.

<sup>8</sup> *La Union del Pueblo Entero v. Abbott*, 751 F. Supp. 3d 673 (W.D. Tex. 2024) (containing the FFCLs regarding First Amendment challenges). Although this order was already published by the time I tested Merlin’s GenAI capabilities, I did not upload it to the secure site before testing in order to avoid introducing bias to the testing.

<sup>9</sup> Merlin used Claude 3.5 Sonnet at the time of testing but is now equipped with a variety of the leading GenAI models.

<sup>10</sup> Of course, even GenAI tools with access to legal databases like Westlaw or LexisNexis are merely starting points for judges and clerks during the legal research process and not a substitute for judicial analysis. That is, even if GenAI accurately identifies the weight of nonbinding authority, I may not be inclined to follow it. See also Magesh et al., *supra* note 4, at 226 (noting that GenAI models designed for legal research have difficulty grasping hierarchies of legal authority).

<sup>11</sup> Since conducting these experiments, I have also had the opportunity to test Westlaw’s AI-assisted research tool for legal research, CoCounsel, and a GenAI platform designed to support judges and their judicial staff called “Learned Hand,” which has recently been adopted by the Michigan Supreme Court. See Press Release, Learned Hand, *The Mich. Sup. Ct. Conts. with Learned Hand for Purpose-Built Jud. AI*, NAT’L L. REV. (Aug. 11, 2025), <https://duke.is/r/w5nt>.

# Two federal judges say use of AI led to errors in US court rulings

By Sara Merken

October 23, 2025 3:29 PM CDT · Updated 19 hours ago



Chairman of the Senate Judiciary Committee Senator Chuck Grassley (R-IA) attends an oversight hearing of U.S. Attorney General Pam Bondi, on Capitol Hill in Washington, D.C., U.S., October 7, 2025. REUTERS/Jonathan Ernst/File Photo [Purchase Licensing Rights](#) 

## Companies



United States Senate

Follow

 Zoom In

Oct 23 (Reuters) - Two federal judges admitted in response to an inquiry by U.S. Senate Judiciary Committee Chairman Chuck Grassley that members of their staff used artificial intelligence to help prepare [recent court orders](#) that Grassley called "error-ridden."

 Reuters AI

...ed by Grassley's office on Thursday, U.S. District Judge Henry Wingate in Mississippi and U.S. District Judge Julien Xavier Neals in New Jersey said the decisions in the unrelated cases did not go through their chambers' typical review processes before they were issued.

The Reuters Daily Briefing newsletter provides all the news you need to start your day. Sign up [here](#).

Both judges said they have since adopted measures to improve how rulings are reviewed.

Neals, based in Newark, in his [letter](#) said a draft decision in a securities lawsuit "was released in error – human error – and withdrawn as soon as it was brought to the attention of my chambers." He said a law school intern used OpenAI's ChatGPT for research without authorization or disclosure.

Neals said his chambers has since created a written AI policy and enhanced its review process. Reuters previously [reported](#) that research produced using AI was included in the decision, citing a person familiar with the circumstances.

Wingate said in his [letter](#) that a law clerk in his court in Jackson used Perplexity "as a foundational drafting assistant to synthesize publicly available information on the docket." He said posting the draft decision "was a lapse in human oversight."

Wingate had removed and replaced the original order in the civil rights lawsuit and previously [declined to give an explanation](#), saying it contained "clerical errors."

The judges did not immediately respond to requests for comment sent to their court staff.

Grassley had [asked the judges to explain](#) whether AI was used in the decisions after lawyers in the cases said they contained factual inaccuracies and other serious errors.

Grassley in a statement on Thursday said he commended the judges for acknowledging the mistakes and urged the judiciary to adopt stronger AI guidelines.

"Each federal judge, and the judiciary as an institution, has an obligation to ensure the use of generative AI does not violate litigants' rights or prevent fair treatment under the law," Grassley said.

Lawyers have also increasingly [faced scrutiny](#) from judges across the country for apparent misuse of AI. Judges have [levied fines or other sanctions](#) in dozens of cases over the past few years after lawyers failed to vet the output the technology generated.

Reporting by Sara Merken; Editing by David Bario and Marguerita Choy

Our Standards: [The Thomson Reuters Trust Principles](#).

Suggested Topics: [Society & Equity](#) [Constitutional Law](#) [Human Rights](#) [Judiciary](#) [Data Privacy](#)

[Purchase Licensing Rights](#)



**Sara Merken**  
Thomson Reuters

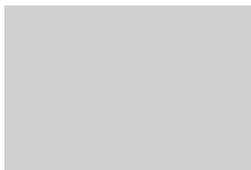


Sara Merken reports on the business of law, including legal innovation and law firms in New York and nationally.

## Read Next



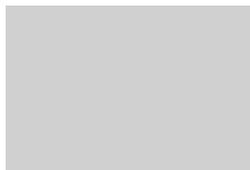
Boards, Policy & Regulation  
**EU finds Meta, TikTok in breach of transparency obligations**



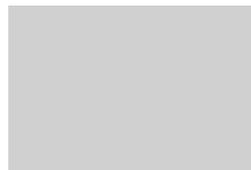
World at Work  
**Target to cut 1,800 corporate roles in turnaround effort**



World  
**EU hits banks, prison medic and Chinese refineries in Russia sanctions**



**Qatar urges gas producers to oppose trade barriers, including EU sustainability law**



Boards, Policy & Regulation  
**Consumers seek \$2.36 billion from Google after privacy verdict**



Boards, Policy & Regulation  
**French court p TotalEnergies greenwashing**

Feedback

Discover the key points from this story with Reuters AI

Try Reuters AI

Reuters AI

## 2 Attys Sanctioned For AI Citations In Pa. Copyright Suit Filing

By **Matt Perez**

Law360 (January 27, 2026, 2:30 PM EST) -- A federal judge in Pennsylvania has reprimanded two attorneys in a copyright infringement suit for filing a motion to dismiss that contained at least eight false case citations generated by artificial intelligence.

The conduct arose from a copyright infringement complaint filed in September by California-based e-commerce retailer Lifetime Well LLC accusing IBSpot.com Inc., a Wyoming corporation doing business principally Pennsylvania, of selling counterfeit Lifetime Well products on IBSpot's website.

Jeffrey J. Goldin, local counsel for IBSpot, and pro hac vice attorney Yen-Yi Anderson were sanctioned Monday after a motion to dismiss filed in November on behalf of IBSpot "offered authorities which did not stand for the propositions asserted, arose from inapposite jurisdictions, or included inaccurate quotations," according to the order. The false citations were caught by lawyers within the court.

"Attorneys are again forewarned. Judges and their talented lawyers in chambers scrutinize memoranda," U.S. District Judge Mark. A. Kearney said in his order. "Submissions containing unverified authority divert limited resources from other litigants who rely on their advocates' careful research, accurate citation, and disciplined advocacy."

Judge Kearney imposed monetary sanctions of \$4,000 against Anderson, who is based in New York City, payable personally to the City Bar Justice Center's Neighborhood Entrepreneur Law Project.

In addition, Anderson must send a cover letter to the director of the project enclosing Monday's order and memorandum, along with a new AI policy instituted at her law firm to share amongst the membership. She is also required to provide a copy of the cover letter and attachments to all counsel and the presiding judges in two other matters.

Goldin in Pennsylvania, meanwhile, was not hit with monetary sanctions but must send a cover letter to the president of the Philadelphia Intellectual Property Lawyers Association enclosing the order, memorandum and his new AI policy to share across the association.

Neither attorney will be referred to their respective state bar disciplinary authorities, the judge said.

"Today's tailored sanction serves more as a lesson to other lawyers who may resort to the easy way hoping to meet economic and time goals," Judge Kearney said. "Goldin erred in ignoring his local counsel obligations."

Anderson responded to accusations of AI use by firing a new lawyer at her office who played a role in preparing the motion to dismiss, according to the order. Anderson did not explain why she did not perform due diligence in a memorandum prepared by an attorney under her supervision, nor did she explain why she did not use the mistake as a lesson rather than a reason to fire the green lawyer.

According to the order, Anderson noted the newly graduated law clerk "seemed entirely reliant on AI to do even the most basic legal research," using Lexis+ AI and LexisNexis Protégé as tools.

"[Anderson] also placed her local co-counsel at risk of sanction without cite checking or reading the cases in the memorandum," Judge Kearney noted. " She asked him to sign and file."

Judge Kearney found both attorneys' conduct violated Rule 11 of the Federal Rules of Civil Procedure, which does not prohibit the use of generative AI, but does require parties verify they are not submitting briefs to the court that rely on fictitious cases.

"We are guided by reasoning from our colleagues across the country addressing misuse of generative artificial intelligence without oversight," Judge Kearney said. "These violations persist despite repeated judicial warnings and extensive public discussion of the risks associated with unverified artificial intelligence-assisted legal research."

In an emailed statement to Law360 Pulse on Tuesday, Goldin said, "I respect the court's ruling and take my professional responsibilities very seriously. The court recognized that I acted promptly once the issue came to light and that I took concrete steps to ensure that this does not happen again. I appreciate the court's measured approach and the opportunity to contribute to broader education and training on the responsible use of technology in the legal practice."

Anderson told Law360 Pulse in a statement Tuesday that, while she notes the case was "satisfactorily resolved last year on behalf of my client" and that she respects Judge Kearney's opinion and will comply with the order, "I am deeply saddened, disappointed, and discouraged by the decision that essentially scapegoats me over my former law clerk's unauthorized and unreported artificial intelligence usage."

She added: "As founder of a tiny firm dedicated to fighting for justice for entrepreneurial business, immigration, and pro bono clients, especially those from East Asia, my clients are often pitted against the federal government or against giant Am Law 200 firms representing companies or individuals with seemingly unlimited resources. This decision only serves as precedent that further disadvantages the little ones battling for survival in a market dominated by huge, institutional, and corporate players."

She concluded: "Nevertheless, my firm and I will learn from this experience as we continue undeterred in seeking justice for the thousands of small businesses and millions of immigrants that support the very fabric of our nation's society, during this time of great need."

Representatives for Lifetime Well did not provide comment Tuesday.

Lifetime Well is represented by Howard N. Shipley and Clair E. Wischusen of Gordon Rees Scully Mansukhani LLP.

IBSpot is represented by Jeffrey J. Goldin of Goldin Law Group PC and Yen-Yi Anderson of Anderson & Associates Law PC.

The case is Lifetime Well LLC v. IBSpot.com Inc., case number 25-5135, in the U.S. District Court for the Eastern District of Pennsylvania.

--Editing by Lakshna Mehta.

*Law360 is owned by LexisNexis Legal & Professional, a RELX company.*



## [Account](#)

News, cases, companies, fir

Try our [Advanced Search](#) for more refined results

News, cases, companies, fir

News, cases, companies, fir

Toggle Dropdown

- [Search Law360](#)
- [Search News Only](#)
- [Search Cases Only](#)
- [Search PTAB Only](#)
- [Search TTAB Only](#)
- [Advanced Search](#)

[s-tenenbaum@law.northw...](#)

- [My Account](#)
- [Emails & Alerts](#)
- [Newsletter Signup](#)
- [My Briefcase](#)
- [Log Out](#)

[Close](#)

- Account
- [My Account](#)
- [My Feeds and Alerts](#)
- [My Briefcase](#)
- [Newsletter Signup](#)
- [Help](#)
- [Log Out](#)
  
- Law360
- [Law360 UK](#)
- [Law360 Pulse](#)

- [Law360 Employment Authority](#)
- [Law360 Tax Authority](#)
- [Law360 Insurance Authority](#)
- [Law360 Real Estate Authority](#)
- [Law360 Healthcare Authority](#)
- [Law360 Bankruptcy Authority](#)
  
- Products
  - [Lexis®](#)
  - [Law360 In-Depth](#)
  - [Law360 Podcasts](#)
  
- Rankings
  - [Leaderboard Analytics](#)
  - [Regional Powerhouses](#)
  - [Law360's MVPs](#)
  - [Women in Law Report](#)
  - [Law360 400](#)
  - [Diversity Snapshot](#)
  - [Practice Groups of the Year](#)
  - [Rising Stars](#)
  - [Titans of the Plaintiffs Bar](#)
  
- Sections
  - [Adv. Search & Platform Tools](#)
  - [About all sections](#)
  - [Browse all sections](#)
  - [Banking](#)
  - [Bankruptcy](#)
  - [Class Action](#)
  - [Competition](#)
  - [Employment](#)
  - [Energy](#)
  - [Expert Analysis](#)
  - [Insurance](#)
  - [Intellectual Property](#)
  - [Product Liability](#)
  - [Securities](#)
  
- Beta Tools
  - [Track docs](#)
  - [Track attorneys](#)
  - [Track judges](#)
  
- Site Menu
  - [Join the Law360 team](#)
  - [Search legal jobs](#)
  - [Learn more about Law360](#)
  - [Read testimonials](#)
  - [Contact Law360](#)
  - [Sign up for our newsletters](#)
  - [Law360 Company](#)
  - [About Law360 Authority](#)
  - [Resource Library](#)
  - [Site Map](#)

What does job satisfaction mean to you?

[Click here to take the Law360 survey.](#)

# AI Docs Sent By Exec To Attys Not Privileged, Judge Says

By [Pete Brush](#) · [Listen to article](#)

*Law360, New York* (February 10, 2026, 12:46 PM EST) -- A Manhattan federal judge said Tuesday that a Texas financial services executive accused of a \$150 million fraud cannot claim privilege over documents that he prepared using an artificial intelligence service and sent to his attorneys — but suggested the materials could be problematic if used at trial.

U.S. District Judge Jed S. Rakoff made the comments from the bench during a morning conference in the run-up to former Beneficient CEO Bradley Heppner's scheduled April 6 trial on charges including fraud and lying to auditors.

Starting around 2018, Heppner, of Dallas, looted GWG Holdings, a publicly traded company he controlled that invested heavily in Beneficient, the Manhattan U.S. attorney's office [charged last year](#). Heppner took millions for himself prior to GWG's bankruptcy, which caused \$1 billion in investor losses, the feds say.

Heppner denies guilt and has argued, among other things, that the indictment unfairly blames him for the bankruptcy.

In 2025, after Heppner knew he was a law enforcement target, he used an unnamed AI tool to prepare 31 documents related to his legal case and shared them with defense counsel from [Quinn Emanuel Urquhart & Sullivan LLP](#), according to filings and statements in court Tuesday.

That gave rise to a government request for the court not to shield the documents under either attorney-client privilege or under the theory that they are protected work product.

Judge Rakoff quickly dispatched the first theory, saying Tuesday, "I'm not seeing remotely any basis for any claim of attorney-client privilege."

On the work-product theory, defense counsel Benjamin O'Neil then argued that the documents incorporate information that Quinn Emanuel conveyed to Heppner.

"It's not as if these were documents created during the course of the alleged scheme," O'Neil said, though he conceded they "were prepared by the defendant of his own volition."

Prosecutor Alexandra Rothman said the documents do not "reflect the legal strategy" of Heppner's defense team.

Judge Rakoff agreed, concluding that the AI documents were not prepared by attorneys.

The judge also noted that the tool used by Heppner contains a provision that any information inputted is not confidential — essentially, that a user has no expectation of privacy.

O'Neil said that if prosecutors try to use the AI-generated information at trial, it could give rise to a "witness-advocate conflict" since his law firm would become a witness in such a scenario.

"That's an interesting point, and you've put the government on notice," Judge Rakoff said. Having defense counsel morph mid-trial into a witness would risk a mistrial, the judge suggested.

Also on Tuesday, Judge Rakoff said he is examining a defense dismissal motion, including an assertion that a count against Heppner of making false statements to auditors should be dismissed because the charged conduct took place in 2019, outside a four-year statute of limitations.

"I'm particularly intrigued by the motion to dismiss Count 4 as time-barred," the judge said.

The sides are due back in court on April 2.

Heppner is represented by Benjamin O'Neil, Christopher Clore, John Scanlon and Robert Zink of Quinn Emanuel Urquhart & Sullivan LLP.

The government is represented by Daniel Nessim and Alexandra Rothman of the [U.S. Attorney's Office for the Southern District of New York](#).

The case is U.S. v. Heppner, case number [1:25-cr-00503](#), in the [U.S. District Court for the Southern District of New York](#).

--Editing by Marygrace Anderson.

*For a reprint of this article, please contact [reprints@law360.com](mailto:reprints@law360.com).*

## 0 Comments

sam tenenbaum

Your name will appear next to your comment. If you do not disclose your full name, your comment will be deleted. Your email address will not be visible to the public.

[Terms of Service](#)

Tell us what you think (1,500 characters max)

Comment

## Attached Documents

- [Motion](#)
- [Memorandum](#)

## Useful Tools & Links

- [Add to Briefcase](#)

- [Save to PDF & Print](#)
- [Rights/Reprints](#)
- [Editorial Contacts](#)

## Related Sections

- [Asset Management](#)
- [Banking](#)
- [Bankruptcy](#)
- [Compliance](#)
- [Corporate](#)
- [Fintech](#)
- [Legal Ethics](#)
- [New York](#)
- [Private Equity](#)
- [Securities](#)
- [Texas](#)
- [White Collar](#)

## Case Information

### Case Title

[USA v. HEPPNER](#)

### Case Number

[1:25-cr-00503](#)

### Court

New York Southern

### Nature of Suit

### Judge

[Jed S. Rakoff](#)

### Date Filed

October 28, 2025

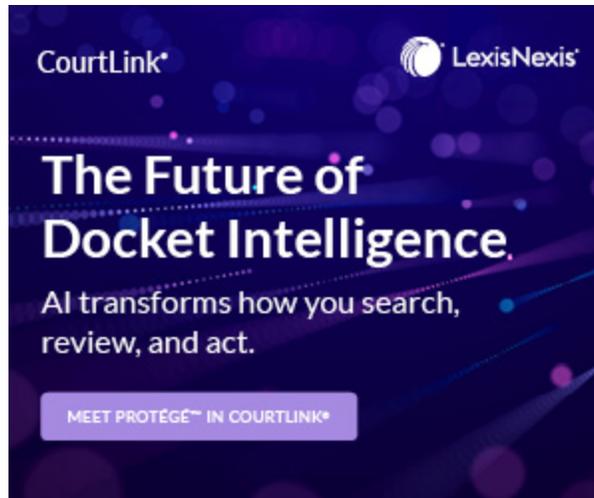
### Law Firms

- [Quinn Emanuel](#)

### Government Agencies

- [U.S. Attorney's Office for the Southern District of New York](#)

- [U.S. District Court for the Southern District of New York](#)



## Judge Analytics

powered by Lex Machina®

- [Jed S. Rakoff](#)

### [Law360 Names Practice Groups Of The Year](#)

Law360 would like to congratulate the winners of its Practice Groups of the Year awards for 2025, which honor the attorney teams behind litigation wins and significant transaction work that resonated throughout the legal industry this past year.

## Top 10 trending in Asset Management

- [1LRN Shareholder To Pay \\$18M To End Del. Defamation Suit](#)
- [2Sentencing Commission's Reform Ideas May Cut Prison Time](#)
- [3Nationwide ERISA 401\(k\) Class Action Heads To Bench Trial](#)
- [4AI Docs Sent By Exec To Attys Not Privileged, Judge Says](#)
- [5State Street Says Kronos Data Breach Cost It \\$27.6M](#)
- [6Tool Co. Can't Escape Workers' 401\(k\) Forfeiture Suit](#)
- [7Catching Up With Delaware's Chancery Court](#)
- [8Fresenius Can't Knock Out 401\(k\) Forfeiture Suit](#)
- [9BlackRock Arm Faces Investor Suit Over Lending Losses](#)
- [10Safanad Sells UK Care Home Biz To REIT For \\$1.6B](#)



Add this article to my briefcase

---

2025



# Practice Groups of the Year

AI Docs Sent By Exec To Attys Not Privileged, Judge Says

New Folder Name - Required

OR SELECT FROM



[Add Now](#)



Sign up for our Asset Management newsletter

You must correct or enter the following before you can sign up:

Please provide a professional email:

[Select more newsletters to receive for free](#)

Law360 takes your privacy seriously. Please see our [Privacy Policy](#).

No Thanks [Sign up now](#)

Thank You!

<https://www.wsj.com/finance/stocks/ai-threatens-a-wall-street-cash-cow-financial-and-legal-data-6782657e>

MARKETS & FINANCE | STOCKS

# AI Threatens a Wall Street Cash Cow: Financial and Legal Data

Stock market losses highlighted expanding risk of AI-driven disruption for financial services and sector's white-collar professionals

By [Alexander Osipovich](#) [Follow](#) and [Ben Dummett](#) [Follow](#)

Feb. 4, 2026 8:14 am ET



Fears about new developments in artificial intelligence swept through the stock market on Tuesday.

RICHARD DREW/AP

## Quick Summary ∨

- Shares of financial data companies like S&P Global and LSEG tumbled this week after Anthropic unveiled new AI tools.

[View more](#)

For years it seemed like a surefire business model: amass vast troves of financial data and sell it to Wall Street for a premium. Then Claude came along.

Shares of companies such as [S&P Global](#), [MSCI](#), [Intercontinental Exchange](#), [London Stock Exchange Group](#) LSEG **-0.42%** ▼ and [FactSet Research Systems](#) FDS **0.27%** ▲

all [tumbled this week](#) after fast-growing artificial-intelligence startup Anthropic unveiled a new suite of tools for automating legal tasks.

The [new legal plug-in](#) for Anthropic's Cowork assistant, powered by its AI model Claude, didn't seem to have much to do with financial data. Nonetheless, LSEG—which has spent years pivoting away from its traditional stock-exchange business to selling data and analytics—slid 13% on Tuesday, and its shares dropped further Wednesday morning.

S&P Global and FactSet were also hit with double-digit losses on Tuesday, while ICE and MSCI both fell more than 5%.

The losses highlighted the expanding threat of AI-driven disruption for financial services and the white-collar professionals who work in the sector.

In recent months, the sophistication of a new Claude-based tool [for writing code](#) rattled software engineers and raised concern about its impact on the broader tech industry. Anthropic's rollout of new legal tools added to similar fears for lawyers and hit the stock of companies that run legal-research databases, such as Thomson Reuters.

The selloff rippled out into a swath of other companies, as investors assessed which businesses are next in line for disruption by AI.

“The market has cast a very broad net as to which companies can be exposed to AI risk,” said UBS analyst Michael Werner. “You don't have to be in the crosshairs of this particular AI risk. You can be in the periphery.”

The rout has expanded to other corners of the software industry, such as outsourcing, where AI tools could reduce the need for human consultants. In India, shares of [Infosys](#) and Tata Consultancy Services both fell around 7% on Wednesday.

The drop this week isn't completely out of the blue. Investors had been souring on the software sector since late last year, months before this week's action. The price of the iShares Expanded Tech-Software Exchange-Traded Fund peaked in September and had slumped by nearly one-quarter before Tuesday.

“Is software dead” is the biggest question that investors should be asking themselves about the fallout from AI, Apollo Asset Management co-president John Zito said at a conference last fall. Apollo has largely been avoiding the software sector for months.

Not everyone thinks the selloff makes sense.

[Nvidia](#) Chief Executive Jensen Huang [said late Tuesday](#) at an [event hosted by Cisco](#) that it makes sense for AI to use existing tools to accomplish tasks, rather than reinventing them. “Would you use a hammer or invent a new hammer?” he asked.

“There’s a whole bunch of software companies whose stock prices are under a lot of pressure because somehow AI is going to replace them,” Huang said. “It is the most illogical thing in the world.”

Financial-data providers might seem like an unlikely target for AI-driven disruption, since many of the biggest ones derive their value from proprietary access to data and information feeds used by bankers and traders.

That had seemed like an impregnable advantage for S&P Global. Besides its well-known credit-ratings business, the New York-based company makes money by selling data products ranging from stock-market indexes to oil-price feeds to insurance-industry analytics.

Its share price soared more than fivefold in the decade ending in 2025, outpacing its own S&P 500 index, which roughly tripled over the same period. So far this year S&P Global is down around 10%, including Tuesday’s losses.

Lucrative opportunities in data attracted exchange operators, which saw subscription-based services as a way to earn stable recurring revenues.

LSEG pursued a [costly acquisition](#) of Refinitiv Holdings in an effort to challenge data-terminal powerhouse Bloomberg. Intercontinental Exchange grew its data business in areas such as bonds, mortgages and even trading signals based on the [chatter in Reddit forums](#).

Spokespeople for LSEG, ICE and S&P Global declined to comment. FactSet and MSCI didn’t immediately respond to requests for comment.

Such companies have argued that, if anything, AI would increase the value of their services, making it easier to extract business insights and trading opportunities from the raw material of their data. Companies with proprietary data feeds say even AI tools must use the underlying information they provide to track the markets.

“AI cannot replicate or replace our real-time data,” LSEG Chief Executive David Schwimmer said in October.

### **Corrections & Amplifications**

Tata Consultancy Services was misspelled as Tata Consulting Services in an earlier

version of this article. (Corrected on Feb. 4)

## Watch: WSJ Interviews Anthropic's CEO in Davos

---

[Alexander Osipovich](#) is a London-based business, finance and economics reporter for The Wall Street Journal. He previously covered exchanges and cryptocurrencies.

Before joining The Wall Street Journal in 2016, he worked for The Moscow Times, Agence France-...



[Ben Dummett](#) writes about dealmaking from The Wall Street Journal's London bureau. His coverage area extends across sectors and regions in EMEA.

Before that he worked in the Journal's Canadian bureau in Toronto where he reported on business an...



---

## Further Reading

**Anthropic Takes Aim at OpenAI's ChatGPT in Super Bowl Ad Debut**

**Are We in an AI Bubble?**

**Microsoft's Pivotal AI Product Is Running Into Big Problems**

# Bill Regulating Attorney AI Use Passes California Senate

By **Emily Sawicki**

Law360 (January 30, 2026, 5:37 PM EST) -- A proposed California law that would regulate attorneys and arbitrators' use of generative artificial intelligence statewide has headed to the Assembly after the state Senate unanimously approved the measure.

In a 39-0 vote Thursday, state senators signed off on the legislation to amend the state's Business and Professions Code and the Code of Civil Procedure to include guidelines for the use of AI in the legal profession, with no formal opposition speaking up against the move.

**Introduced** Jan. 5, the bill requires lawyers to ensure that no confidential or nonpublic information is entered into a public AI system. It also mandates that lawyers review any material created by AI to verify its accuracy, and remove any harmful or biased content.

The bill also prohibits arbitrators from relying on generative AI to analyze or decide on matters that come before them, stating in part that arbitrators "shall not delegate any part of their decision-making process to any generative artificial intelligence tool" and "shall avoid delegating any tasks to generative artificial intelligence tools if such use could influence procedural or substantive decisions."

Known as Senate Bill 574, the legislation was authored by state Sen. Tom Umberg, a Democrat representing Orange County.

"I'm pleased to see SB 574 moving forward," Umberg said in a statement on Friday. "As AI becomes more common in the legal system, we need clear guardrails to protect clients' confidentiality and ensure that real people, not algorithms, are making legal decisions."

--Editing by Patrick Reagan.

*Update: This article was updated with a statement from state Sen. Tom Umberg.*



Sections

BU TODAY

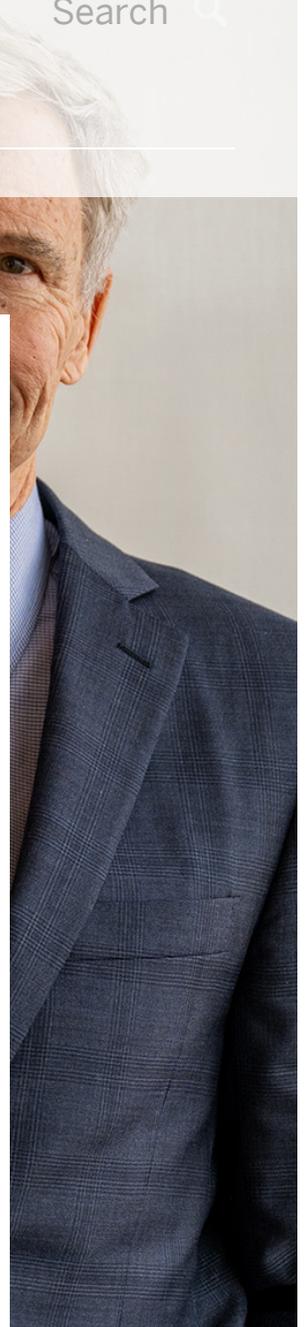
Search

News, Research, Community

UNIVERSITY NEWS

# New AI Program Keeps BU School of Law Students on the Cutting Edge

**Initiative led by LAW's Timothy Duncan is designed to provide the curriculum, training, and tools necessary for students to learn how to use artificial intelligence skillfully now and in the future**



*AI is something that amplifies and expands capabilities that people already have, says Timothy Duncan, a LAW lecturer and director of the new BU LAW AI Program.*

---

January 15, 2026



SHARE THIS

---

Like any tool, artificial intelligence is as good—as useful, as creative, as efficient—as the person using it. For those in the legal profession, whose jobs require carefully sifting and synthesizing thousands, even hundreds of thousands, of pages of documents, AI could be a game changer. The Boston University School of Law is training the next generation of lawyers to be leaders in this change.

LAW's new AI Program is designed to provide the curriculum, training, and tools necessary for students to learn how to use artificial intelligence skillfully and wisely, preparing them for the AI-enabled legal practice of the future. [Timothy Duncan](#), a LAW lecturer whose teaching includes the intersection of law, technology, and regulation, with a focus on artificial intelligence, has been appointed the program's inaugural director.

“AI is something that amplifies and expands capabilities that people already have,” Duncan says. “A good metaphor for me is electric bikes: the harder you pedal, the more it helps you. AI is an extension of yourself in many ways—including, which I think most people overlook, creativity. Lawyers need to be creative in terms of looking at fact patterns and issues and coming up with approaches to litigation. So I think that AI can be very helpful in terms of thinking about things, creating ideas, and then also evaluating and critiquing different things that you might come up with.”

The AI program is still in its early stages, he says, but plans include bringing artificial intelligence directly into the classroom



“With Tim’s leadership, BU LAW is positioned to be at the forefront of legal education in the age of AI,” says [Angela Onwuachi-Willig](#), dean of LAW and Ryan Roth Gallo Professor of Law. “This program reflects our commitment to equipping our students not just with knowledge of the law, but also with the tools and judgment to practice it in a world transformed by technology.”

Already the School of Law is hosting a series of monthly faculty training and information sessions, and in October the school [launched a partnership](#) with [Harvey](#), a leading provider of domain-specific generative artificial intelligence designed for legal and professional services. BU is one of 18 schools—including the University of Chicago, University of Pennsylvania, NYU, University of Michigan, Stanford, and Vanderbilt, among others—to partner with Harvey to bring genAI tools directly to law students and faculty.

“People talk about AI replacing lawyers, or replacing a good deal of their work, but I don’t think that’s going to happen,” Duncan says. “I do think lawyers will not be able to get a job in five years unless they’re proficient at using different AI tools, because AI stands to make lawyers much more productive and efficient. I tell my students that there’s a great opportunity right now to get in on the ground floor. We’re seeing this with students who graduated last year and have some proficiency and understanding in AI—they’re getting appointed to AI committees at their companies.”

He sees AI as merely the latest in a line of technology that has changed the legal profession throughout his career, which has included a tenure as head of technology at the former Consumer Financial Protection Bureau under President Barack Obama, as



“My entire career, I’ve been interested in technology. And my career really spans that period of time when technology changed the practice of law and continues to change the practice of law,” Duncan says. “Think about personal computers and the internet—I don’t think technology really impacted the practice of law for the 150 years before them, and now we’re in another period of big change with AI. It’s exciting, and it’s interesting to understand how these technologies can help lawyers be more creative and more effective.”

**EXPLORE RELATED TOPICS:**

[ARTIFICIAL INTELLIGENCE](#) [FACULTY](#) [LAW](#) [SCHOOL OF LAW](#) [STUDENTS](#)

---

*Share this story*

---

**Latest from BU Today.**

**TIPS FOR STUDENTS**

A Guide for CGS Students: How to Kickstart Your BU Experience

Lady Gaga, Mister Rogers Revive Memories of Iconic BU Commencement Moment

**TERRIER SPIRIT DAYS**

First Terrier Spirit Day Is February 5—Wear Your BU Gear

**VARSITY SPORTS**

Men’s Hockey Terriers Out to Defend Their Reigning Beanpot Title

---