

TEAM 1 – KENNEDY INN OF COURT – MCLE HANDOUT*

Showdown at the AI Corral: Evidence at the Cultural and Technological Frontier

I. ABA FORMAL OPINION 512 – Covering the Growing Use of Generative Artificial Intelligence (attached separately as a pdf)

- Lawyers must have a reasonable understanding of the capabilities and limitations of generative AI to meet the competence requirements under Model Rule 1.1. They are required to independently verify the outputs provided by AI tools, as failing to do so could result in a violation of this rule. For instance, if an AI is used to review and summarize lengthy contracts, a lawyer does not need to manually review each document as long as they have previously verified the tool's accuracy with a smaller set of documents. However, AI cannot be used to offer legal advice, negotiate claims, or perform other functions that require personal judgment or active participation from the lawyer. Additionally, lawyers must be mindful of their clients' confidentiality, adhering to Model Rules 1.6, 1.9(c), and 1.18(b). This means assessing the risk of unauthorized access or disclosure of client information when using AI, given that AI's self-learning capabilities could potentially expose client data to unauthorized third parties. Therefore, informed consent from clients is necessary before their information is inputted into AI tools. While it is not required for lawyers to disclose every research tool used, if AI research is crucial to the outcome of a case, clients must be informed that AI was utilized. According to Model Rule 8.4(c), lawyers must avoid conduct involving dishonesty, fraud, deceit, or misrepresentation. Consequently, attorneys must ensure that AI-generated citations are accurate, analyses are correct, and arguments are not misleading to avoid deceiving the court. Furthermore, attorneys should establish policies to ensure that their employees use AI properly. When billing, if AI takes 15 minutes to create a memorandum, only 15 minutes should be billed. Charging a flat fee for AI use might be unreasonable if certain aspects of a client's case do not require AI assistance.
- [ABA issues first ethics guidance on a lawyer's use of AI tools \(americanbar.org\)](https://www.americanbar.org/publications/aba_formal_opinion/2021/07/2021-07-01-512/)

II. The State Bar of California, Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law (attached separately as a pdf)

- [Practical Artificial Intelligence in the Practice of Law](https://www.sbcabar.org/practical-artificial-intelligence-in-the-practice-of-law)

III. Advisory Committee on Evidence Rules:

Extract from April 2024 (not saved as an attached pdf due to the file size – use link below to access)

[2024-04_agenda_book_for_evidence_rules_meeting_final.pdf \(uscourts.gov\)](https://www.uscourts.gov/2024-04_agenda_book_for_evidence_rules_meeting_final.pdf)

- The Grimm-Grossman Proposal on Amendments to FRE 901
 - [901](b) Examples. The following are examples only—not a complete list—of evidence that satisfies the requirement [of Rule 901(a)]:
 - (9) Evidence about a Process or System. For an item generated by a process or system:
 - (A) evidence describing it and showing that it produces an accurate a valid and reliable result; and
 - (B) if the proponent concedes that the item was generated by artificial intelligence, additional evidence that:
 - (i) describes the software or program that was used; and
 - (ii) shows that it produced valid and reliable results in this instance.
 - Proposed New Rule 901(c) to address “Deepfakes” 901(c): Potentially Fabricated or Altered Electronic Evidence. If a party challenging the authenticity of computer-generated or other electronic evidence demonstrates to the court that it is more likely than not either fabricated, or altered in whole or in part, the evidence is admissible only if the proponent demonstrates that its probative value outweighs its prejudicial effect on the party challenging the evidence.
 - The rules governing evidence, including the authenticity rule, can be adapted to address AI with only minor updates. As our society evolves, so too should our legal standards. Paul W. Grimm and Maura R. Grossman propose that only slight modifications to existing rules are necessary to handle AI-generated evidence effectively. Since AI-generated evidence would fall under Rule 901, which pertains to evidence produced by a process or system, the authenticity rules can still apply. Furthermore, implementing an additional requirement, such as the "reverse balancing" test found in Rule 609, would enhance confidence that only authentic evidence is admitted, ensuring that any misleading or fabricated evidence is excluded.

IV. STATUTES & CASES

Applicable California Statute:

California Penal Code § 1054.1

The prosecuting attorney shall disclose to the defendant or his or her attorney all of the following materials and information, if it is in the possession of the prosecuting attorney or if the prosecuting attorney knows it to be in the possession of the investigating agencies:

- (a) The names and addresses of persons the prosecutor intends to call as witnesses at trial.
- (b) Statements of all defendants.
- (c) All relevant real evidence seized or obtained as a part of the investigation of the offenses charged.
- (d) The existence of a felony conviction of any material witness whose credibility is likely to be critical to the outcome of the trial.
- (e) Any exculpatory evidence.
- (f) Relevant written or recorded statements of witnesses or reports of the statements of witnesses whom the prosecutor intends to call at the trial, including any reports or statements of experts made in conjunction with the case, including the results of physical or mental examinations, scientific tests, experiments, or comparisons which the prosecutor intends to offer in evidence at the trial.

Applicable Cases:

Berger v. U.S. (1935) 295 U.S. 78.

- This case involved a prosecuting attorney who used improper methods during a witness's cross-examination, including making assumptions to mislead the jury. The main issue was whether the prosecutor's behavior—particularly his comments and actions—had deprived the defendant of a fair trial.
- The Supreme Court ruled that the prosecutor's conduct violated the defendant's right to a fair trial. This case emphasizes that all defendants have the right to a fair trial and ensures that attorneys are not out of line when representing people in court.
- “It is as much his duty to refrain from improper methods calculated to produce a wrongful conviction as it is to use every legitimate means to bring about a just one.” (88)
- “[T]he United States prosecuting attorney overstepped the bounds of that propriety and fairness which should characterize the conduct of such an officer in the prosecution of a criminal offense is clearly shown by the record.” (84)

Tennison v. City & County of San Francisco (9th Cir. 2008) 570 F.3d 1078, 1087.

- Both the Ninth Circuit and the Supreme Court have recognized that “exculpatory evidence cannot be kept out of the hands of the defense just because the prosecutor does not have it, where an investigating agency does.”

People v. Riel (Cal. 2000) 998 P.2d 969.

- “Presenting incredible evidence may raise difficult tactical decisions but, as long as counsel has no specific undisclosed factual knowledge of its falsity, it does not raise an ethical problem.” citing Criminal Law section 443.
- Attorneys are prohibited from presenting evidence they know to be false or from facilitating known frauds on the court. However, they can ethically present evidence if they suspect but do not have personal knowledge, that it is false.

United States v. Young (1985) 470 U.S. 1, 25-26.

- The Court’s “invited error” analysis, which suggests that prosecutorial misconduct may be excused if it merely responds to defense misconduct by “righting the scale,” is fundamentally flawed and undermines ethical standards for federal prosecutors (ante, at 1045). This approach neglects the higher ethical obligations of government representatives, as emphasized in *Berger v. United States*, and contradicts the Court’s own acknowledgment that such misconduct is erroneous (ante, at 1043, 1046). The suggestion that misconduct could be deemed “reasonable” or “necessary” contradicts the principle that improper prosecutorial conduct should not be permitted or justified under any circumstances (ante, at 1045, 1046).

Kyles v. Whitley (1995) 514 U.S. 419, 438.

- The Supreme Court emphasized that the prosecution can’t avoid its responsibility to disclose favorable evidence by making judgment calls about its importance.

United States v. Chu (9th Cir. 1993) 5 F.3d 1244, 1249.

- The responsibility to seek justice requires lawyers representing the United States “to see that all evidence relevant to the case is presented, even if unfavorable to its position.”

Brady v. Maryland (1947) 373 U.S. 83, 87.

- While the government’s disclosure obligation encompasses more than just exculpatory evidence, the failure to produce evidence “material either to guilt or punishment” gives rise to constitutional violations. *Brady* at 87. A prosecutor who withholds such evidence violates not only his disclosure obligations but also the due process clause. *Id.* Due process is violated “irrespective of the good faith or bad faith of the prosecution.” *Id.*

V. California Rules of Professional Conduct

1.1 Competence ([Rule of Professional Conduct 1.1 \(ca.gov\)](#))

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

1.4 Communications ([Rule 1.4 \[3-500\] \(2023\) \(ca.gov\)](#))

(a) A lawyer shall:

- (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
- (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
- (3) keep the client reasonably informed about the status of the matter;
- (4) promptly comply with reasonable requests for information; and
- (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

1.6: Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

- (1) to prevent reasonably certain death or substantial bodily harm;
- (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
- (3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
- (4) to secure legal advice about the lawyer's compliance with these Rules;
- (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;
- (6) to comply with other law or a court order; or
- (7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

1.9(c): Duties to Former Clients ([Rule 1.9-Exec Summary-Redline.pdf \(ca.gov\)](#))

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:

- (1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or
- (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.

1.18(b): Duties to Prospective Client ([Rule 1.18-Exec Summary-Redline.pdf \(ca.gov\)](#))

(b) Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information, except as Rule 1.9 would permit with respect to information of a former client.

3.1: Meritorious Claims & Contentions ([Rule 3.1-Exec Summary-Redline.pdf \(ca.gov\)](#))

A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous, which includes a good faith argument for an extension, modification or reversal of existing law. A lawyer for the defendant in a criminal proceeding, or the respondent in a proceeding that could result in incarceration, may nevertheless so defend the proceeding as to require that every element of the case be established.

3.3: Candor Towards the Tribunal ([Rule 3.3-Exec Summary-Redline.pdf \(ca.gov\)](#))

(a) A lawyer shall not knowingly:

- (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
- (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
- (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

3.8: Special Responsibilities of a Prosecutor ([Rule 3.8.pdf \(ca.gov\)](#))

The prosecutor in a criminal case shall:

- (a) refrain from prosecuting a charge that the prosecutor knows is not supported by probable cause;
- (b) make reasonable efforts to assure that the accused has been advised of the right to, and the procedure for obtaining, counsel and has been given reasonable opportunity to obtain counsel;
- (c) not seek to obtain from an unrepresented accused a waiver of important pretrial rights, such as the right to a preliminary hearing;
- (d) make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and, in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal;
- (e) not subpoena a lawyer in a grand jury or other criminal proceeding to present evidence about a past or present client unless the prosecutor reasonably believes:
 - (1) the information sought is not protected from disclosure by any applicable privilege;
 - (2) the evidence sought is essential to the successful completion of an ongoing investigation or prosecution; and
 - (3) there is no other feasible alternative to obtain the information;
- (f) except for statements that are necessary to inform the public of the nature and extent of the prosecutor's action and that serve a legitimate law enforcement purpose, refrain from making extrajudicial comments that have a substantial likelihood of heightening public condemnation of the accused and exercise reasonable care to prevent investigators, law enforcement personnel, employees or other persons assisting or associated with the prosecutor in a criminal case from making an extrajudicial statement that the prosecutor would be prohibited from making under Rule 3.6 or this Rule.
- (g) When a prosecutor knows of new, credible and material evidence creating a reasonable likelihood that a convicted defendant did not commit an offense of which the defendant was convicted, the prosecutor shall:
 - (1) promptly disclose that evidence to an appropriate court or authority, and
 - (2) if the conviction was obtained in the prosecutor's jurisdiction,
 - (i) promptly disclose that evidence to the defendant unless a court authorizes delay, and
 - (ii) undertake further investigation, or make reasonable efforts to cause an investigation, to determine whether the defendant was convicted of an offense that the defendant did not commit.

(h) When a prosecutor knows of clear and convincing evidence establishing that a defendant in the prosecutor's jurisdiction was convicted of an offense that the defendant did not commit, the prosecutor shall seek to remedy the conviction.

ABA Model Rule of Professional Conduct 3.8 comment (1984).

- "A prosecutor has a responsibility of a minister of justice and not simply that of an advocate."

5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers ([Rule 5.1-Exec Summary-Redline.pdf \(ca.gov\)](#))

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

- (1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
- (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

8.4: Misconduct ([Rule 8.4-Exec Summary-Redline.pdf \(ca.gov\)](#))

It is professional misconduct for a lawyer to:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;

(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

(d) engage in conduct that is prejudicial to the administration of justice;

(e) state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law;

(f) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law; or

(g) engage in conduct that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, marital status or socioeconomic status in conduct related to the practice of law. This paragraph does not limit the ability of a lawyer to accept, decline or withdraw

from a representation in accordance with Rule 1.16. This paragraph does not preclude legitimate advice or advocacy consistent with these Rules.

VI. Secondary Sources (attached as PDFs)

Law360 Article dated 8/21/24 by Phillip Bantz – “How AI Could Shake Up Federal Evidence Rules”

New York Times Article dated 8/14/24 by Stuart A. Thompson – “How ‘Deep Fake Elon Musk’ Became the Internet’s Biggest Scammer”

***The Anthony M. Kennedy Inn of Court certifies that this activity has been approved for MCLE credit by the State Bar of California.**

##

**THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT**

**PRACTICAL GUIDANCE FOR THE USE OF
GENERATIVE ARTIFICIAL INTELLIGENCE IN THE PRACTICE OF LAW**

EXECUTIVE SUMMARY

Generative AI is a tool that has wide-ranging application for the practice of law and administrative functions of the legal practice for all licensees, regardless of firm size, and all practice areas. Like any technology, generative AI must be used in a manner that conforms to a lawyer’s professional responsibility obligations, including those set forth in the Rules of Professional Conduct and the State Bar Act. A lawyer should understand the risks and benefits of the technology used in connection with providing legal services. How these obligations apply will depend on a host of factors, including the client, the matter, the practice area, the firm size, and the tools themselves, ranging from free and readily available to custom-built, proprietary formats.

Generative AI use presents unique challenges; it uses large volumes of data, there are many competing AI models and products, and, even for those who create generative AI products, there is a lack of clarity as to how it works. In addition, generative AI poses the risk of encouraging greater reliance and trust on its outputs because of its purpose to generate responses and its ability to do so in a manner that projects confidence and effectively emulates human responses. A lawyer should consider these and other risks before using generative AI in providing legal services.

The following Practical Guidance is based on current professional responsibility obligations for lawyers and demonstrates how to behave consistently with such obligations. While this guidance is intended to address issues and concerns with the use of generative AI and products that use generative AI as a component of a larger product, it may apply to other technologies, including more established applications of AI. This Practical Guidance should be read as guiding principles rather than as “best practices.”

PRACTICAL GUIDANCE

Applicable Authorities	Practical Guidance
<p>Duty of Confidentiality</p> <p>Bus. & Prof. Code, § 6068, subd. (e)</p> <p>Rule 1.6</p> <p>Rule 1.8.2</p>	<p>Generative AI products are able to utilize the information that is input, including prompts and uploaded documents or resources, to train the AI, and might also share the query with third parties or use it for other purposes. Even if the product does not utilize or share inputted information, it may lack reasonable or adequate security.</p> <p>A lawyer must not input any confidential information of the client into any generative AI solution that lacks adequate confidentiality and security protections. A lawyer must anonymize client information and avoid entering details that can be used to identify the client.</p> <p>A lawyer or law firm should consult with IT professionals or cybersecurity experts to ensure that any AI system in which a lawyer would input confidential client information adheres to stringent security, confidentiality, and data retention protocols.</p> <p>A lawyer should review the Terms of Use or other information to determine how the product utilizes inputs. A lawyer who intends to use confidential information in a generative AI product should ensure that the provider does not share inputted information with third parties or utilize the information for its own use in any manner, including to train or improve its product.</p>
<p>Duties of Competence and Diligence</p> <p>Rule 1.1</p> <p>Rule 1.3</p>	<p>It is possible that generative AI outputs could include information that is false, inaccurate, or biased.</p> <p>A lawyer must ensure competent use of the technology, including the associated benefits and risks, and apply diligence and prudence with respect to facts and law.</p> <p>Before using generative AI, a lawyer should understand to a reasonable degree how the technology works, its limitations, and the applicable terms of use and other policies governing the use and exploitation of client data by the product.</p> <p>Overreliance on AI tools is inconsistent with the active practice of law and application of trained judgment by the lawyer.</p> <p>AI-generated outputs can be used as a starting point but must be carefully scrutinized. They should be critically analyzed for</p>

Applicable Authorities	Practical Guidance
	<p>accuracy and bias, supplemented, and improved, if necessary. A lawyer must critically review, validate, and correct both the input and the output of generative AI to ensure the content accurately reflects and supports the interests and priorities of the client in the matter at hand, including as part of advocacy for the client. The duty of competence requires more than the mere detection and elimination of false AI-generated results.</p> <p>A lawyer’s professional judgment cannot be delegated to generative AI and remains the lawyer’s responsibility at all times. A lawyer should take steps to avoid over-reliance on generative AI to such a degree that it hinders critical attorney analysis fostered by traditional research and writing. For example, a lawyer may supplement any AI-generated research with human-performed research and supplement any AI-generated argument with critical, human-performed analysis and review of authorities.</p>
<p>Duty to Comply with the Law</p> <p>Bus. & Prof. Code, § 6068(a)</p> <p>Rule 8.4</p> <p>Rule 1.2.1</p>	<p>A lawyer must comply with the law and cannot counsel a client to engage, or assist a client in conduct that the lawyer knows is a violation of any law, rule, or ruling of a tribunal when using generative AI tools.</p> <p>There are many relevant and applicable legal issues surrounding generative AI, including but not limited to compliance with AI-specific laws, privacy laws, cross-border data transfer laws, intellectual property laws, and cybersecurity concerns. A lawyer should analyze the relevant laws and regulations applicable to the attorney or the client.</p>
<p>Duty to Supervise Lawyers and Nonlawyers, Responsibilities of Subordinate Lawyers</p> <p>Rule 5.1</p> <p>Rule 5.2</p> <p>Rule 5.3</p>	<p>Managerial and supervisory lawyers should establish clear policies regarding the permissible uses of generative AI and make reasonable efforts to ensure that the firm adopts measures that give reasonable assurance that the firm’s lawyers and non lawyers’ conduct complies with their professional obligations when using generative AI. This includes providing training on the ethical and practical aspects, and pitfalls, of any generative AI use.</p> <p>A subordinate lawyer must not use generative AI at the direction of a supervisory lawyer in a manner that violates the subordinate lawyer’s professional responsibility and obligations.</p>

Applicable Authorities	Practical Guidance
<p>Communication Regarding Generative AI Use</p> <p>Rule 1.4</p> <p>Rule 1.2</p>	<p>A lawyer should evaluate their communication obligations throughout the representation based on the facts and circumstances, including the novelty of the technology, risks associated with generative AI use, scope of the representation, and sophistication of the client.</p> <p>The lawyer should consider disclosure to their client that they intend to use generative AI in the representation, including how the technology will be used, and the benefits and risks of such use.</p> <p>A lawyer should review any applicable client instructions or guidelines that may restrict or limit the use of generative AI.</p>
<p>Charging for Work Produced by Generative AI and Generative AI Costs</p> <p>Rule 1.5</p> <p>Bus. & Prof. Code, §§ 6147–6148</p>	<p>A lawyer may use generative AI to more efficiently create work product and may charge for actual time spent (e.g., crafting or refining generative AI inputs and prompts, or reviewing and editing generative AI outputs). A lawyer must not charge hourly fees for the time saved by using generative AI.</p> <p>Costs associated with generative AI may be charged to the clients in compliance with applicable law.</p> <p>A fee agreement should explain the basis for all fees and costs, including those associated with the use of generative AI.</p>
<p>Candor to the Tribunal; and Meritorious Claims and Contentions</p> <p>Rule 3.1</p> <p>Rule 3.3</p>	<p>A lawyer must review all generative AI outputs, including, but not limited to, analysis and citations to authority for accuracy before submission to the court, and correct any errors or misleading statements made to the court.</p> <p>A lawyer should also check for any rules, orders, or other requirements in the relevant jurisdiction that may necessitate the disclosure of the use of generative AI.</p>
<p>Prohibition on Discrimination, Harassment, and Retaliation</p> <p>Rule 8.4.1</p>	<p>Some generative AI is trained on biased information, and a lawyer should be aware of possible biases and the risks they may create when using generative AI (e.g., to screen potential clients or employees).</p> <p>Lawyers should engage in continuous learning about AI biases and their implications in legal practice, and firms should establish policies and mechanisms to identify, report, and address potential AI biases.</p>

Applicable Authorities	Practical Guidance
Professional Responsibilities Owed to Other Jurisdictions Rule 8.5	A lawyer should analyze the relevant laws and regulations of each jurisdiction in which a lawyer is licensed to ensure compliance with such rules.

July 29, 2024

ABA issues first ethics guidance on a lawyer's use of AI tools

Share:



CHICAGO, July 29, 2024 — The American Bar Association Standing Committee on Ethics and Professional Responsibility released today its first formal opinion covering the growing use of generative artificial intelligence (GAI) in the practice of law, pointing out that model rules related to competency, informed consent, confidentiality and fees principally apply.

Formal Opinion 512 states that to ensure clients are protected, lawyers and law firms using GAI must “fully consider their applicable ethical obligations,” which includes duties to provide competent legal representation, to protect client information, to communicate with clients and to charge reasonable fees consistent with time spent using GAI.

“This opinion identifies some ethical issues involving the use of GAI tools and offers general guidance for lawyers attempting to navigate this emerging landscape,” the formal opinion said. It added that the ABA committee and state and local bar association ethics committees will likely continue to “offer updated guidance on professional conduct issues relevant to specific GAI tools as they develop.”

The 15-page opinion specifically outlined that lawyers should be mindful of a host of model rules in the [ABA Model Rules of Professional Conduct](#), including:

- Model Rule 1.1 (Competence). This obligates lawyers to provide competent representation to clients and requires they exercise the “legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” In addition, the model rule states

lawyers should understand “the benefits and risks associated” with the technologies used to deliver legal services to clients.

- Model Rule 1.6 (Confidentiality of Information). Under this model rule, a lawyer using GAI must be cognizant of the duty to keep confidential all information relating to the representation of a client, regardless of its source, unless the client gives informed consent. Other model rules require lawyers to extend similar protections to former and prospective clients’ information.
- Model Rule 1.4 (Communications). This model rule addresses lawyers’ duty to communicate with their clients and builds on lawyers’ legal obligations as fiduciaries, which include “the duty of an attorney to advise the client promptly whenever he has any information to give which it is important the client should receive.” Of particular relevance to GAI, Model Rule 1.4(a)(2) states that a lawyer shall “reasonably consult” with the client about the means by which the client’s objectives are to be accomplished.
- Model Rule 1.5 (Fees). This rule requires a lawyer’s fees and expenses to be reasonable and includes criteria for evaluating whether a fee or expense is reasonable. The formal opinion notes that if a lawyer uses a GAI tool to draft a pleading and expends 15 minutes to input the relevant information into the program, the lawyer may charge for that time as well as for the time necessary to review the resulting draft for accuracy and completeness. But, in most circumstances, the lawyer cannot charge a client for learning how to work a GAI tool.

“With the ever-evolving use of technology by lawyers and courts, lawyers must be vigilant in complying with the Rules of Professional Conduct to ensure that lawyers are adhering to their ethical responsibilities and that clients are protected,” Formal Opinion 512 concluded.

The standing committee periodically issues ethics opinions to guide lawyers, courts and the public in interpreting and applying ABA model ethics rules to

specific issues of legal practice, client-lawyer relationships and judicial behavior. Other recent ABA ethics opinions are available [here](#).

The ABA is the largest voluntary association of lawyers in the world. As the national voice of the legal profession, the ABA works to improve the administration of justice, promotes programs that assist lawyers and judges in their work, accredits law schools, provides continuing legal education, and works to build public understanding around the world of the importance of the rule of law. View our [privacy statement](#) online. Follow the latest ABA news at www.americanbar.org/news and on X (formerly Twitter) [@ABANews](#).



How 'Deepfake Elon Musk' Became the Internet's Biggest Scammer

An A.I.-powered version of Mr. Musk has appeared in thousands of inauthentic ads, contributing to billions in fraud.



By Stuart A. Thompson Aug. 14, 2024

All Steve Beauchamp wanted was money for his family. And he thought Elon Musk could help.

Mr. Beauchamp, an 82-year-old retiree, saw a video late last year of Mr. Musk endorsing a radical investment opportunity that promised rapid returns. He contacted the company behind the pitch and opened an account for \$248. Through a series of transactions over several weeks, Mr. Beauchamp drained his retirement account, ultimately investing more than \$690,000.

Then the money vanished — lost to digital scammers on the forefront of a new criminal enterprise powered by artificial intelligence.

ADVERTISEMENT



Gartner® names Twilio a Leader in CPaaS Positioned highest for ability to execute

The scammers had edited a genuine interview with Mr. Musk, replacing his voice with a replica using A.I. tools. The A.I. was sophisticated enough that it could alter minute mouth movements

to match the new script they had written for the digital fake. To a casual viewer, the manipulation might have been imperceptible.

“I mean, the picture of him — it was him,” Mr. Beauchamp said about the video he saw of Mr. Musk. “Now, whether it was A.I. making him say the things that he was saying, I really don’t know. But as far as the picture, if somebody had said, ‘Pick him out of a lineup,’ that’s him.”

Thousands of these A.I.-driven videos, known as deepfakes, have flooded the internet in recent months featuring phony versions of Mr. Musk deceiving scores of would-be investors. A.I.-powered deepfakes are expected to contribute to billions of dollars in fraud losses each year, according to estimates from Deloitte.

The videos cost just a few dollars to produce and can be made in minutes. They are promoted on social media, including in paid ads on Facebook, magnifying their reach.

“It’s probably the biggest deepfake-driven scam ever,” said Francesco Cavalli, the co-founder and chief of threat intelligence at Sensity, a company that monitors and detects deepfakes.

The videos are often eerily lifelike, capturing Mr. Musk’s iconic stilted cadence and South African accent.

Original



Audio

Original

A.I.

Scammers will start with a genuine video, like this interview from The Wall Street Journal conducted by Thorold Barker, an editor whose voice is also heard in the clip.

Mr. Musk's mouth movements are edited with lip-synching technology, which tweaks how someone speaks. Scammers will add an A.I. voice using voice-cloning tools, which

copies any voice from sample clips.

The final ad, which can include fake graphics mimicking news organizations, can be quite

convincing for casual internet users._

Source: The Wall Street Journal (original clip)

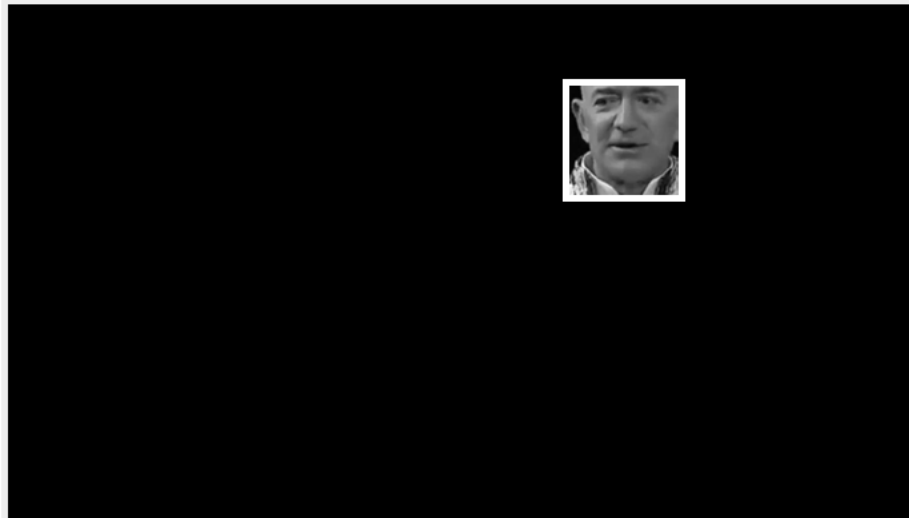
Mr. Musk was by far the most common spokesperson in the videos, according to Sensity, which analyzed more than 2,000 deepfakes.

He was featured in nearly a quarter of all deepfake scams since late last year, Sensity found. Among those focused on cryptocurrencies, he was featured in nearly 90 percent of the videos.

The deepfake ads also featured Warren Buffett, the prominent investor, and Jeff Bezos, the founder of Amazon, among others.

Mr. Musk did not respond to requests for comment.

Altered by A.I.



A.I.

Original

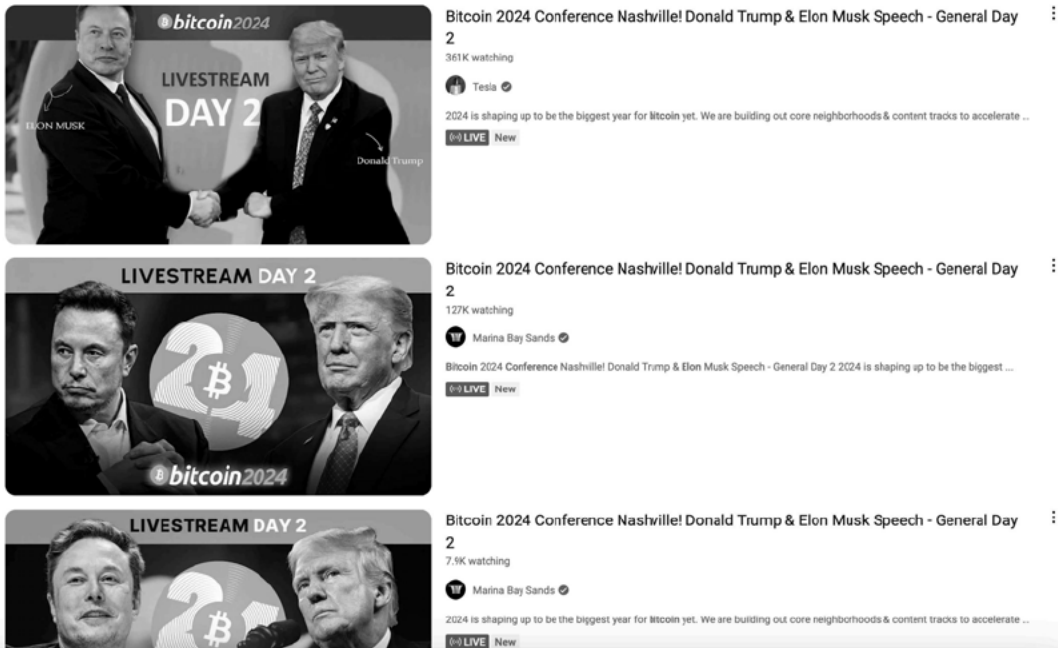
Prime Video India (original clip)

It is difficult to quantify exactly how many deepfakes are floating online, but a search of Facebook's ad library for commonly used language that advertised the scams uncovered hundreds of thousands of ads, many of which included the deepfake videos. Though Facebook has already taken down many of them for violating its policies and disabled some of the accounts that were responsible, other videos remained online and more seemed to appear each day.

YouTube was also flooded with the fakes, often using a label that suggests the video is "live." In fact, the videos are prerecorded deepfakes.

'Live' YouTube Scams

Search results on YouTube for "Elon Bitcoin conference" showed dozens of supposedly live videos featuring a deepfake Mr. Musk hawking crypto scams. Some videos were watched by hundreds of thousands of people.



YouTube

After former President Donald J. Trump spoke at a Bitcoin conference Saturday, YouTube hosted dozens of videos using the “live” label that showed a prerecorded deepfake version of Elon Musk saying he would personally double any cryptocurrency sent to his account. Some of the videos had hundreds of thousands of viewers, though YouTube said scammers can use bots to artificially inflate the number.

One Texan said he lost \$36,000 worth of Bitcoin after seeing an “impersonation” of Mr. Musk speaking on a so-called live YouTube video in February 2023, according to a report with the Better Business Bureau, the nonprofit consumer advocacy group.

“I send my bitcoin, and never got anything back,” the person wrote.

Altered by A.I.



Source: CNET (original clip)

YouTube said in a statement that it had removed more than 15.7 million channels and over 8.2 million videos for violating its guidelines from January to March of this year, with most of those violating its policies against spam.

The prevalence of the phony ads prompted Andrew Forrest, an Australian billionaire whose videos were also used to create deepfake ads on Facebook, to file a civil lawsuit against Meta, its parent company, for negligence in how its ad business is run. He claimed that Facebook's advertising business lured "innocent users into bad investments."

Meta, which owns Facebook, said the company was training automated detection systems to catch fraud on its platform, but also described a cat-and-mouse game where well-funded scammers constantly shifted their tactics to evade detection.

YouTube pointed to its policies prohibiting scams and manipulated videos. The company in March made it a requirement that creators disclose when they use A.I. to create realistic content.

ADVERTISEMENT



Limited-Time Fall Offer

Sponsored By Paramount+

The internet is now rife with similar reports from people scammed out of thousands of dollars, some of them losing their life savings. Hong Kong's Securities and Futures Commission issued a warning in May about scams featuring Mr. Musk. Earlier this year, the Federal Trade Commission and the Federal Bureau of Investigation warned Americans that A.I.-powered cybercrime and deepfake scams were on the rise.

"Criminals are leveraging A.I. as a force multiplier" in ways that make "cyberattacks and other criminal activity more effective and harder to detect," the F.B.I. said in an emailed statement.

Digital scams are as old as the internet itself. But the new-wave deepfakes featuring Mr. Musk emerged last year after sophisticated A.I. tools were released to the public, allowing anyone to clone celebrity voices or manipulate videos with eerie accuracy. Pornographers, meme-makers and, increasingly, scammers took notice.

'Deepfake Elon Musk'

Thousands of ads circulating online feature an A.I. version of Elon Musk hawking cryptocurrency products or promising large returns on investments.

Altered by A.I.



A.I.

Original

Altered by A.I.



A.I.

Original

Altered by A.I.



A.I.

Original

Sources: TED Talks (first and second videos); Fox News (third video)

“It’s shifting now because organized crime has figured out, ‘we can make money at this,’” according to Lou Steinberg, the founder of CTM Insights, a cybersecurity research lab. “So we’re going to see more and more of these fake attempts to separate you from your money.”

The A.I.-generated videos are hardly perfect. Mr. Musk can sound robotic in some videos and his mouth does not always line up with his words. But they appear convincing enough for some targets of the scam — and are improving all the time, experts said.

Such videos cost as little as \$10 to create, according to Mr. Cavalli from Sensity. The scammers — based mostly in India, Russia, China and Eastern Europe — cobble together the fake videos using a mix of free and cheap tools in less than 10 minutes.

“It works,” Mr. Cavalli said. “So they’ll keep amplifying the campaign, across countries, translating into multiple languages, and continuously spreading the scam to even more targets.”

Some of the scams often advertise phony A.I.-powered software, with claims that they can produce incredible returns on an investment. Targets are encouraged to send a small sum at first — about \$250 — and are slowly lured into investing more as scammers claim that the initial investment is increasing in value.

In one video, taken from a shareholder meeting at Tesla, the deepfake Mr. Musk explains a product for automated trading powered by A.I. that can double a given investment each day.

Altered by A.I.



A.I.

Original

Source: Tesla (original clip)

Experts who have studied crypto communities said Mr. Musk's unique global fanbase of conservatives, anti-establishment types and crypto enthusiasts are often drawn to alternative paths for earning their fortunes — making them perfect targets for the scams.

“There's definitely a group of people who believe that the secret to wealth is being hidden from them,” said Molly White, a researcher who has studied crypto communities. They think that “if they can find the secret to it, then that's all they need.”

ADVERTISEMENT

Scammers often target older internet users who may be familiar with cryptocurrency, A.I. or Mr. Musk, but unfamiliar with the safest ways to invest.

“The elderly have always been a very scammable, profitable population,” said Finn Brunton, a professor of science and technology studies at the University of California, Davis, who is an expert in the crypto market. He added that the elderly had been targets of fraud long before platforms like Facebook made them easier to scam.

Mr. Beauchamp, who is a widower and worked until he was 75 as a sales representative at a company in Ontario, Canada, came across an ad shortly after joining Facebook in 2023. Though he remembers seeing the video live on CNN, a spokeswoman for CNN said Mr. Musk had not appeared for an interview in years. (The New York Times could not identify a video matching Mr. Beauchamp's description, but he said his story was nearly identical to that of another woman scammed online by a deepfaked Mr. Musk.)

He sent \$27,216 last December to a company calling itself Magna-FX, according to emails between Mr. Beauchamp and the company that were shared with The New York Times. Magna-FX made it seem like his investment was increasing in value. At one point, a sales agent used software to take control of Mr. Beauchamp's computer, moving funds around to apparently invest them.

To withdraw the money, Mr. Beauchamp was told to pay a \$3,500 administration fee and another \$3,500 commission fee. He sent the money only to be told that he needed to pay \$20,000 to release a portion of the funds — about \$200,000. He paid that, too.

ADVERTISEMENT

Though Mr. Beauchamp told the scammers that he had exhausted his retirement savings, maxed out his credit cards, tapped a line of credit and borrowed money from his sister to invest and pay the fees, the scammers wanted more. They asked him to pay yet another fee. Mr. Beauchamp contacted the police.

Most traces of Magna-FX were taken offline, including the company website, phone number and email addresses used by the agents Mr. Beauchamp spoke with. Another company bearing a nearly identical name and advertising similar services did not respond to requests for comment.

“I guess now is the time to call me dumb, stupid, idiot and what other superlatives you can think of,” Mr. Beauchamp wrote in a report filed to the Better Business Bureau.

Mr. Beauchamp said he was managing to pay his bills using a smaller retirement account that he had not shared with the scammers, along with his pensions. He had planned to travel the world during his retirement.

Mr. Beauchamp filed a report with the local police but little movement has been made on the case, he said.

“Because of the amount of fraud that is going on everywhere, my case got put in a queue,” he said. “I’m not getting my hopes up.”

How AI Could Shake Up Federal Evidence Rules

By **Phillip Bantz**

Law360 (August 21, 2024, 4:55 PM EDT) -- Judges, lawyers and academics say it's **only** a matter of time before the breakneck development of artificial intelligence collides with a cautious, slow-moving judicial system and gives rise to a thorny array of evidentiary issues. They're just not sure what to do about it.

"This is in the very early stage right now, and there are lots of disagreements," U.S. District Judge Patrick Schiltz of Minneapolis told Law360.

You can place almost anything in doubt. It gives you plausible deniability to say, 'That's not me,' for anything.



Maura Grossman

University of Waterloo, Maura Grossman Law

He chairs the U.S. Judicial Conference's Advisory Committee on Evidence Rules, a panel that has been grappling with proposals to change the evidence rules in reaction to AI-related dangers, including digitally altered images and audio known as deepfakes.

Defendants falsely claiming that real evidence against them has been fabricated or manipulated through generative AI presents another challenge.

"You can place almost anything in doubt. It gives you plausible deniability to say, 'That's not me,' for anything," said Maura Grossman, an e-discovery lawyer in Buffalo, New York, and research professor at the Cheriton School of Computer Science at the University of Waterloo.

Then there's the issue of authenticating AI evidence and assessing the reliability of AI tools used to analyze evidence.

"Another problem is defining what AI even is," said Judge Schiltz, of the District of Minnesota. "I haven't seen a definition yet that made me say, 'Yeah, that will work.'"

He added, "I don't know anything about technology. I would say most judges don't really know much about technology. So there's a lot of **education** that has to go on."

Proposed Rule Changes

Judge Schiltz said the evidence rules committee's focus on AI is a reaction, in part, to U.S. Chief Justice John Roberts writing in his 2023 year-end report on the federal judiciary that AI has "great potential," but also risks "dehumanizing the law."

As AI evolves, courts will need to consider its proper uses in litigation. In the federal courts, several Judicial Conference Committees — including those dealing with court administration and case management, cybersecurity, and the rules of practice and procedure, to name just a few — will be involved in that effort.



John G. Roberts

Chief Justice of the United States

"As AI evolves, courts will need to consider its proper uses in litigation," the chief justice said in the report. "In the federal courts, several judicial conference committees — including those dealing with court administration and case management, cybersecurity and the rules of practice and procedure, to name just a few — will be involved in that effort."

The evidence rules committee has held two conferences with experts on AI and evidentiary issues and will revisit the subject when it reconvenes in November, according to Judge Schiltz.

Judge Schiltz's term as chair of the evidence rules committee expires at the end of September and his successor, U.S. District Judge Jesse

M. Furman of Manhattan, will take over Oct. 1. Judge Furman, a former federal prosecutor for the Southern District of New York, did not respond to an interview request.

Among the proposals on the table is a new rule on challenging potential deepfake evidence. Challengers would have to show the court not only that a jury "reasonably could find that the evidence has been altered or fabricated, in whole or in part," but also that the evidence's "probative value outweighs its prejudicial effect."

"You're going to have to raise meaningful doubt about the veracity of the evidence," Grossman told Law360.

She and former U.S. District Judge Paul Grimm of the District of Maryland, director of Duke Law School's Bolch Judicial Institute, drafted the proposed new rule, which is a revised version of an earlier proposal that the committee rejected.

The previous version would have required a challenger to convince the court that the evidence in question "more likely than not was fake." The committee believed that put too heavy a burden on the challenger, Judge Grimm said in an interview.

The new rule is an attempt to establish a fair balancing test to prevent or at least dissuade defendants from falsely alleging that evidence is a deepfake — frivolous claims that threaten to cast doubt on the legitimacy of evidence across the board while also preventing fake AI evidence from tainting a jury.

"Right now, there is no real procedure for challenging a deepfake," and the current evidence rules "tilt strongly in favor of letting the evidence go to the jury. But once that happens, it becomes very hard to unring the bell," Grossman said.

Judge Grimm added, "Oftentimes, these deepfakes are so dramatic and impactful that if you let the jury see it to decide if it's real or not, the damage is already done."

Proposed New Rule 901(c) to address "deepfakes"

901(c): Potentially Fabricated or altered electronic evidence.

If a party challenging the authenticity of computer-generated or other electronic evidence demonstrates to the court that a jury reasonably could find that the evidence has been altered or fabricated, in whole or in part, the evidence is admissible only if the proponent demonstrates that its probative value outweighs its prejudicial effect on the party challenging the evidence.

He and Grossman also plan to submit to the committee a revised proposal to amend a rule on authenticating evidence "generated by a process or system," which they say covers AI tools.

Under the rule they're drafting, the person seeking to admit the AI-generated evidence would have to detail the "training data and software or program that was used" and show that "they produced valid and reliable results in this instance."

Daniel Capra, a professor at Fordham Law School and a reporter for the evidence rules committee, is working on another draft of a proposed new rule, which would treat "machine-generated evidence" the same as evidence testified to by a human witness.

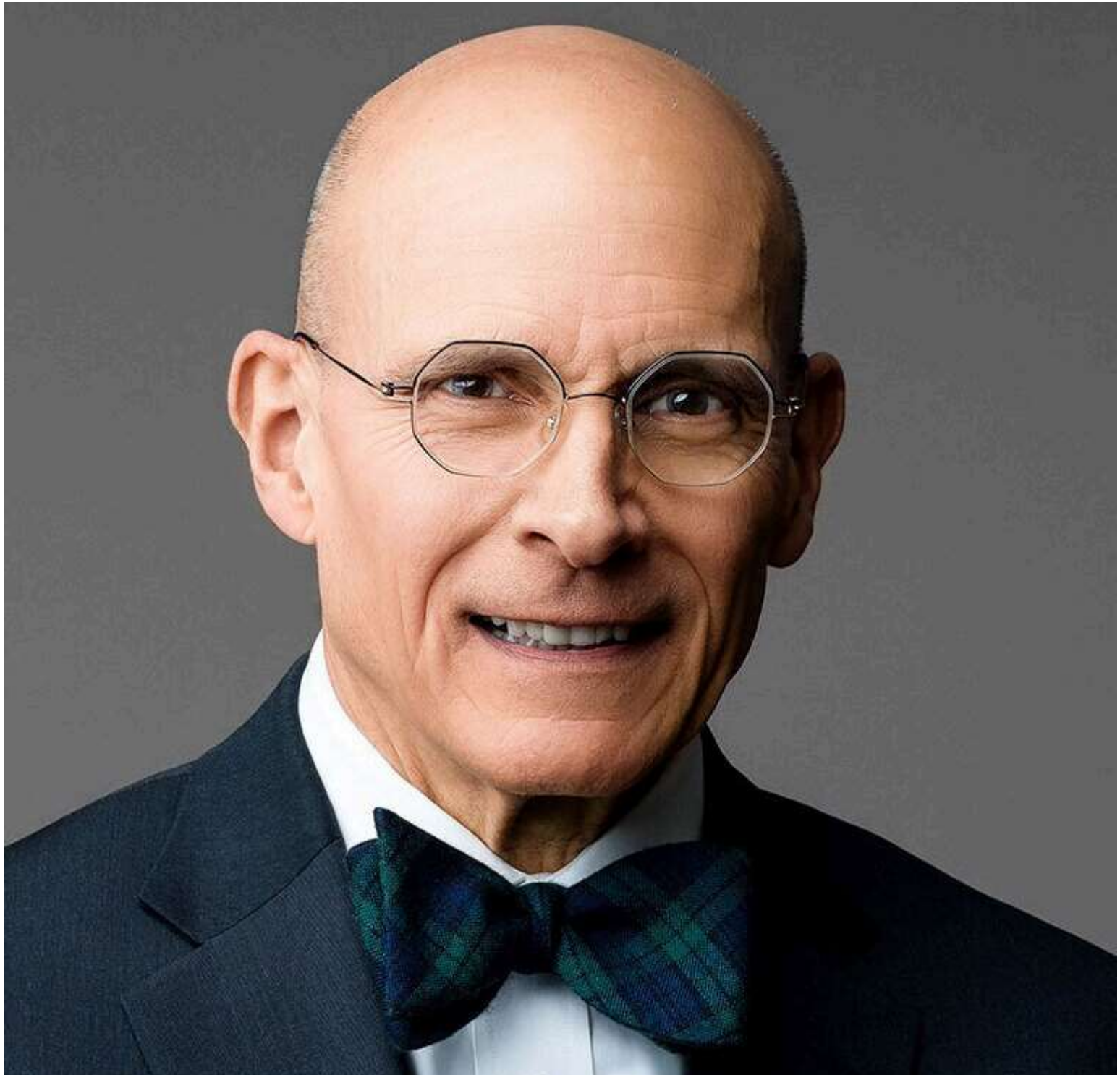
"The idea is that you would have to have a Rule 702 hearing, what's called a Daubert hearing, and the proponent of the evidence would have to call witnesses to verify that the methodology is appropriate and they relied on the proper databases and so forth," Capra told Law360.


The proposed new rule, he added, "is really intended to treat machine-based learning the same way you would treat testimony from live witnesses."

Others who have weighed in during the evidence rule committee's meetings have questioned whether the evidence rules need to be changed at all to deal with AI. They contend that the existing rules are sufficient to deal with AI evidence and point to how the courts adapted to authenticating evidence from social media, according to Judge Schiltz.

When social media was taking off, the evidence rules committee faced calls to take action but opted to sit back and see how things played out in the federal courts, which has worked out relatively well.

Oftentimes, these deepfakes are so dramatic and impactful that if you let the jury see it to decide if it's real or not, the damage is already done.





Paul Grimm

Director of Duke Law School's Bolch Judicial Institute, Retired federal judge for the District of Maryland
The courts ended up using common law authority to essentially graft a requirement on the rules to require anyone challenging the veracity of evidence pulled from social media to "make some sort of showing that they have a legitimate concern about the legitimacy of the evidence," Judge Schiltz said.

That's a similar approach to what Judge Grimm and Grossman have put forth in their proposed new deepfake evidence rule.

"The rules, as they exist, are flexible and the courts are inventive, and the question is whether we actually need text language to help the courts do what they're going to do anyway," Capra said.

AI Evidence Creeps Into Courts

Examples of AI-related evidentiary issues popping up in courtrooms are relatively uncommon at this point. But it's happening.

In March, a Washington state judge made headlines when he rejected a defense attorney's attempt to use AI-enhanced cellphone video in a triple murder case stemming from a fight outside a bar.

Judge Leroy McCullough held in his novel ruling that the AI evidence "would lead to a confusion of the issues and a muddling of eyewitness testimony, and could lead to a time-consuming trial within a trial about the non-peer-reviewable process used by the AI model, such that any relevance is substantially outweighed by the danger of unfair prejudice."

The judge's ruling highlights what Anna Gressel, New York-based litigation counsel at Paul Weiss Rifkind Wharton & Garrison LLP who focuses on AI and digital technology, described to Law360 as growing "concern among the courts about how to discern what might be AI-manipulated or AI-generated."

In white collar crime cases, generative AI tools could be used to create deepfake voice recordings, bogus financial records and other potentially incriminating evidence.

"It's only a matter of time before these AI tools are used in white collar cases, because they are complex and have a lot of data and moving points," said Sean Shecter, co-chair of the white collar practice at Lewis Brisbois Bisgaard & Smith LLP.

He added, "This is 'Brave New World' stuff."

Joel Cohen, chair of White & Case LLP's white collar practice group, told Law360 that he had had cases recently in which "documents that were turned over by a regulator appeared to have been altered" based on a review of the underlying data, or metadata, embedded in the records.

The documents in question included financial records and were the subject of U.S. Department of Justice and Securities and Exchange Commission investigations, according to Cohen.

"It's just a reflection of the enhanced availability of tools that allow even amateurs to do this," he said.

Rule Change Happens Slowly

The earliest that any of the proposed AI-related evidence rules could be enacted would be around 2028, according to Capra. During that time, AI could evolve beyond the scope of the rule changes, once again leaving the courts playing catch-up.

"There's also disagreement about whether it's even possible to do anything, because AI is developing so rapidly that if you write rules that are too specific, they will quickly become outdated," Judge Schiltz said.

"But if you write rules that are too general, they'll basically be useless," he added. "So there's an additional problem of how quickly the technology is changing."

Rule changes occur slowly and deliberately by design under the Rules Enabling Act, which gives the U.S. Supreme Court the authority to amend or create evidence rules. First, though, the rules must make it through the committee, then the Judicial Conference, which sends the proposed changes to the high court.

If the Supreme Court approves the rule it gets sent to Congress, which has about seven months to enact or reject the proposed changes. If Congress does nothing, the rule becomes enacted on its own under the Rules Enabling Act.

For now, though, potential AI rule changes are waiting at the starting line with an uncertain finish several years away.

"Judges are going to have to decide these cases without rules specifically designed to help them do that," Judge Grimm said.

--Editing by Karin Roberts.