Christian Legal Society National Conference
Denver, Colorado, October 9, 2026

AI, DEMOCRACY, AND THE RULE OF LAW

L.O. Natt Gantt, II
Richard M. Campanelli

SECTION 1: AI, Ethics, and Human Dignity

I. Current United States Approach to Regulation of Artificial Intelligence

A. Trump Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence – The White House*, January 23, 2025, "With the right Government policies, we can solidify our position as the global leader in AI and secure a brighter future for all Americans. This order revokes certain existing AI policies and directives that act as barriers to American AI innovation…." See also America's AI Action Plan.

B. USG Comments on AI Governance at UN Security Council September 2025: US "totally reject[s] all efforts by international bodies to assert centralized control and global governance of AI. We believe that the responsible diffusion of AI will help pave the way to a flourishing future, one of increased productivity, empowered individuals, and revolutions in scientific advancement."

C. Promoting Advanced Artificial Intelligence Innovation and Security – The White House, June 2, 2026: Trump Administration responds to potential national security threats arising from anticipated releases of new AI models, particularly Anthropic's April 2026 intended release of Mythos, which effectively identifies vulnerabilities in existing software systems. The White House Executive Order adopts a voluntary compliance approach: "Nothing in this section shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models."

II. Artificial Intelligence Defined

A. The legal definition of AI is evolving. Current frameworks generally characterize AI as computer systems that perform tasks requiring human-like intelligence; however, a precise, universally accepted legal definition has yet to emerge, leading to regulatory challenges. The emerging definition of AI comes from current regulatory frameworks, including various pronouncements from the USG (e.g., the Biden Executive Order on AI, issued October 30, 2023, and such as the European Union Artificial Intelligence (EU AI) Act, formally adopted by the European Council on May 21, 2024.

B. United States

1. Definition: Biden Executive Order on AI defines AI as: "A machine-based system that can, for a given set of human-defined objectives, make predictions,

recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."

2. This definition underscores the role of AI in automating decision-making processes based on inputs from real and virtual environments. The Executive Order also introduces several specific terms related to AI, such as:

(1) AI Model—A component that uses computational statistical or machine-learning techniques to produce outputs.

(2) Generative AI—AI models that generate synthetic content, such as images, videos, audio, and text (see more below).

C. The European Union (EU)

1. The EU AI Act defines AI broadly, encompassing a range of techniques and applications. *T* emphasizes risk-based regulation, categorizing AI applications into four risk levels: unacceptable risk, high risk, limited risk, and minimal risk. This categorization guides the regulatory requirements and obligations for developers and deployers of AI systems. According to the Act, AI systems are defined as:

a) Machine Learning: Including supervised, unsupervised, and reinforcement learning, using a wide variety of methods including deep learning.

b) Logic and Knowledge-Based Approaches: Including expert systems, logic programming, and knowledge representation.

c) Statistical Approaches: Including Bayesian estimation, search, and optimization methods.

2. However, in 2026, the EU announced it was revising its approach to enhance development and application, 2026 Report: Extended Summary for Policymakers | International AI Safety Report.

D. Regarding other relevant statements of law and policy, the G7 Hiroshima AI Process, launched in May 2023, emphasizes a comprehensive policy framework for AI governance, recognizing the importance of trustworthy and responsible AI. It highlights the roles of various stakeholders, including governments, private sector, and civil society, in promoting safe and secure AI development and deployment. *See also* PRC State Council Guidance/AI Action Plan, August 26, 2025, Opinions of the State Council on Deepening the Implementation of the "Artificial Intelligence+" Initiative | Center for Security and Emerging Technology.

III. The Advance of Generative AI. Since the emergence of generative AI at the end of 2022, lawyer attitudes to AI adoption have gone from sporadic curiosity to common usage, to competitive necessity and differentiator.

A. For many years lawyers have used forms of AI in their law practice. For instance, commonly used online research programs use AI in finding results to research queries. Specifically, AI works to extract information responsive to the user's query from a large set of existing data on which the program has been trained.

B. The release of OpenAI's ChatGPT on November 30, 2022, exploded the use and popularity of *generative* AI. This technology goes beyond earlier forms of AI to generate products (such as textual responses or images) in response to a user's request based again on the large set of existing data on which the program has been trained. This generated content is designed to resemble human-created content. Below is a basic explanation of how it works.

1. Basic Concept: Generative AI works by learning patterns from existing data and then using that knowledge to generate new, similar data. This process is like an artist who studies many paintings and then creates a new painting inspired by what they have learned.
    a. Key Components
        i. Training Data: Generative AI starts with a large dataset of examples. For instance, if the goal is to generate realistic images of cats, the AI would be trained on thousands of images of cats.
        ii. Machine Learning Model: The heart of Generative AI is a machine learning model, typically a type of neural network. A neural network is a set of algorithms designed to recognize patterns, similar to how a human brain works.
        iii. Learning Patterns: During training, the model analyzes the training data to learn important features and patterns. For example, it learns what makes a cat look like a cat – ears, whiskers, fur texture, etc.
    b. Generating New Content: After training, the model can create new content that looks like the training data but is not a copy of any specific example. For instance, it can generate a new image of a cat that is unique but has all the characteristics of the cats from which it learned.
    c. Another formulation of this process divides generative AI functionality into two phrases.
        i. Training Phase
            1. Collect Data: Gather a large corpus of text (e.g., all the articles on Wikipedia).
            2. Process Data: Convert the text into a format the AI can understand, typically numerical values representing words or phrases.
            3. Train the Model: Use a neural network (like GPT, generative pre-trained transformer) to process this text data. The model learns the probability of words following each other.
        ii. Generation Phase:
            1. Input a Prompt: Start with an initial text input, like "Once upon a time."
            2. Predict Next Word: The model predicts the next word based on the patterns it learned during training.

3. Iterate: Use the new word as part of the input and predict the next word, and so on, generating a full sentence or paragraph.

IV. Examples of Generative AI Programs/Software in Lawyering

Because the use of generative AI in lawyering is continually evolving, a detailed catalog of the AI tools lawyers are using is out-of-date soon after its compilation. With this caveat, lawyers are using these tools in the following areas:

A. Legal document generation and drafting: ChatGPT, Claude, CoCounsel, Harvey AI, Juro, Loio, Spellbook
B. Legal research assistance: Lexis+ AI (Protégé), Westlaw Precision AI-Assisted Research, vLex Vincent AI, Fastcase
C. Contract review and analysis: Icertis, LawGeex, Kira Systems, Luminance, Spellbook
D. Litigation support and e-discovery: CoCounsel, Everlaw, Relativity
E. Legal predictive analytics: Lex Machina, Premonition, Bloomberg Law Litigation Analytics
F. Compliance and risk management: Ayfie, Icertis, DocuSign Intelligent Insights
G. Legal writing assistance: ChatGPT, Claude, Grammarly, Writer, Harvey AI

V. Ethical Issues Related to the Use of AI

Although AI technology continues to change rapidly, this technology implicates the same ethical duties, such as competence, diligence, confidentiality, proper supervision, and independent professional judgment, that apply to lawyers' use of other forms of technology. Perhaps most notably, lawyers using generative AI must consider the same ethical implications as if they were overseeing another nonlawyer completing legal tasks.

A. <u>Competence & Diligence</u>

1. The ABA Model Rules and many state rules of professional conduct expressly provide that lawyers' general duties of competence extend to their use of technology like artificial intelligence. Lawyers who use AI must understand the "benefits and risks" associated with such technology. ABA Model Rule 1.1[8]; Virginia Rule 1.1[6]. Lawyers therefore cannot avoid considering using AI if it would benefit their practice. Moreover, if they use the technology, they cannot claim ignorance and must know how the technology works and how it can result in ethical problems. Ethics opinions acknowledge that lawyers and law firms often will need to rely on consultants generally in the use of technology but caution that in doing so the lawyers must still ensure ethical standards are satisfied. *See* ABA Formal Opinion 495 - Lawyers Working Remotely (December 16, 2020); ABA Formal Opinion 498 - Virtual Practice (March 10, 2021).

2. For AI, an important related ethical issue concerns what is known as the "black box" challenge. Specifically, when lawyers submit questions to AI-powered tools, the questions go into a "black box" and the AI tools provide an answer. The question then arises how much do competent lawyers using the technology need to know about what

happens inside the "black box." As further discussed in this outline, such AI tools, for instance, may have biases that inhibit their ability to produce good answers.

3. Related to competence, lawyers' ethical duty diligence requires them to exercise "reasonable diligence" in representing a client. ABA Model Rule 1.3. Reasonable diligence, in turn, requires that lawyers do not rely so heavily on AI tools that they fail to provide the proper human oversight to ensure adequate client representation.

4. Relevant Rules of Professional Conduct

> ABA Model Rule 1.1: Competence
> *Client-Lawyer Relationship*
> Rule 1.1 Competence
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
> Maintaining Competence
> [8] 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 (emphasis added).
> Rule 1.3: Diligence
> A lawyer shall act with reasonable diligence and promptness in representing a client.
>
> Virginia Rule 1.1: Competence
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
> *Maintaining Competence*
> [6] To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. Attention should be paid to the benefits and risks associated with relevant technology. . . . (emphasis added).

B. Confidentiality

1. The ABA Model Rules and many state rules of professional conduct expressly provide that lawyers' duty of confidentiality requires they undertake "reasonable efforts" to prevent the disclosure of confidential client information. This duty applies to lawyers' submission of confidential information to AI programs like ChatGPT, Claude, and Gemini for lawyering projects and to concerns over whether such information is improperly disclosed in training the AI or though through data breaches or improper commingling of client data. (Note that these concerns also related to potential implications on the attorney-client privilege.)
2. In many ways, the confidentiality concerns regarding lawyers' use of these services relates to lawyers' use of cloud storage of client information, in which an outside vendor maintains the files.

3. Lawyers thus must take "reasonable" precautions to ensure confidentiality of client information in their use of AI programs. ABA and state rules outline in their comments, as noted below, several factors used in assessing the reasonableness of the lawyers' precautions. The comments to Virginia Rule of Professional Conduct 1.6, in particular, provide detailed information on steps lawyers should consider taking to protect confidential client information.
4. In a context analogous to AI programs, ABA Formal Opinion 498 provides detailed guidance on the considerations necessary to ensure the protection of a client's files and communications through a vendor who provides cloud storage. Specifically, ABA Formal Opinion 498 states: "If the access to such 'files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer."' ABA Formal Op. 498 (quoting ABA Formal Op. 482).
5. In outlining these reasonable steps, the opinion adds that the lawyer must take steps to ensure the vendor regularly backs up any client data stored with the vendor. The lawyer must also ensure other lawyers and nonlawyers the lawyer supervises and any relevant vendors understand the requirements necessary to protect confidential information. ABA Formal Op. 498.
6. Relevant Rules of Professional Conduct

> ABA Model Rule 1.6: Confidentiality of Information
> (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.
> [18] Paragraph (c) 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. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. *Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and 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).* 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 that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4]. (emphasis added)

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

North Carolina Rule 1.6: Confidentiality of Information

(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.

Acting Competently to Preserve Confidentiality

[19] Paragraph (c) requires a lawyer to act competently to safeguard information acquired during 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. See Rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information acquired during the professional relationship with a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. *Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and 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).* 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 that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information to comply with other law—such as state and federal laws that govern data privacy, or that impose notification requirements upon the loss of, or unauthorized access to, electronic information—is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4]. (emphasis added)

[20] When transmitting a communication that includes information acquired during the representation of a client, the lawyer must take reasonable

precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the client's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Virginia Rule 1.6: Confidentiality of Information

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule.

[20] Paragraph (d) makes clear that a lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information. Perfect online security and data protection is not attainable. Even large businesses and government organizations with sophisticated data security systems have suffered data breaches. Nevertheless, security and data breaches have become so prevalent that some security measures must be reasonably expected of all businesses, including lawyers and law firms. Lawyers have an ethical obligation to implement reasonable information security practices to protect the confidentiality of client data. *What is "reasonable" will be determined in part by the size of the firm. See Rules 5.1(a)-(b) and 5.3(a)-(b). The sheer amount of personal, medical and financial information of clients kept by lawyers and law firms requires reasonable care in the communication and storage of such information. A lawyer or law firm complies with paragraph (d) if they have acted reasonably to safeguard client information by employing appropriate data protection measures for any devices used to communicate or store client confidential information.*

To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer can and more likely must turn to the expertise of staff or an outside technology professional. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well.

[21] Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:

(a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;

(b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;

(c) Procedures addressing security measures for access of third parties to stored information;
(d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;
(e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and
(f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity. (emphasis added)

C. Duty of Supervision

1. With the rise of AI, much legal commentary has already been devoted to how AI systems, particularly generative AI, can perform certain legal tasks that junior lawyers and paraprofessionals, like paralegals, have traditionally performed. Lawyers' ethical duty of supervision therefore applies to AI-powered tools.
2. Lawyers have duties in ABA Model Rules 5.1 and 5.3, and their state counterparts, to supervise lawyers and nonlawyers properly. The relevant rule in this context is Rule 5.3 regarding nonlawyer supervision and, in pertinent part, requires lawyers to "make reasonable efforts" to ensure that actions in which AI engages are "compatible with the professional obligations of the lawyer."

> ABA Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistance
> With respect to a nonlawyer employed or retained by or associated with a lawyer:
> (a) a partner, 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 the person's conduct is compatible with the professional obligations of the lawyer;
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the 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 person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

D. Unauthorized Practice of Law

1. Related to lawyers' duty to supervise nonlawyers properly is the duty that lawyers cannot ethically delegate certain tasks to a nonlawyer and cannot assist a nonlawyer in the unauthorized practice of law. See ABA Model Rule 5.5. At the same time, as noted above, lawyers' duty of competence and diligence

encourages lawyers not to "under-delegate" tasks to AI when such delegation would improve their provision of legal services.[1]

2. "One way of framing this issue is automation versus augmentation," states Dr. Tonya Custis, a Research Director at Thomson Reuters who leads a team of research scientists developing natural-language and search technologies for legal research. "There may be some tasks that we shouldn't automate. For these tasks, AI can help attorneys do their jobs, but AI can't do their jobs completely. So the question becomes: where do we draw that line?"[2]
3. Regarding the prohibition against lawyers' assisting others in the unauthorized practice of law (UPL), the relevant rules provide:

> ABA Model Rule 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law (emphasis added)
> (a) A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, *or assist another in doing so.*
> [2] The definition of the practice of law is established by law and varies from one jurisdiction to another. Whatever the definition, limiting the practice of law to members of the bar protects the public against rendition of legal services by unqualified persons. This Rule does not prohibit a lawyer from employing the services of paraprofessionals and delegating functions to them, so long as the lawyer supervises the delegated work and retains responsibility for their work. See Rule 5.3.
>
> Virginia Rule 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law (emphasis added)
> (c) A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or *assist another in doing so*.
> [2] The definition of the practice of law is established by law and varies from one jurisdiction to another. Whatever the definition, limiting the practice of law to members of the bar protects the public against rendition of legal services by unauthorized persons. Paragraph (c) does not prohibit a lawyer from employing the services of paraprofessionals and delegating functions to them, so long as the lawyer supervises the delegated work and retains responsibility for their work. *See* Rule 5.3.

4. An interesting AI development related to UPL is "legal chatbots." These are "AI-powered programs that interact with users who have legal issues by simulating a conversation or dialogue. These chatbots are now being used to . . . perform such tasks as fight parking tickets, advise victims of crimes, or draft privacy policies or non-disclosure agreements."[3] One such chatbot is DoNotPay. According to its website, "DoNotPay is an artificial intelligence chatbot that helps consumers fight corporations, beat bureaucracy, find hidden money, and

[1] *See* David Lat, *The Ethical Implications of Artificial Intelligence*, at https://abovethelaw.com/law2020/the-ethical-implications-of-artificial-intelligence/?rf=1 (last visited June 5, 2026).
[2] *Id*.
[3] *Id*.

protect their rights. The chatbot was created by British entrepreneur Joshua Browder in 2015 to help people appeal parking tickets. It has since expanded to help users with over 1,000 consumer issues and tasks." DoNotPay - Your AI Consumer Champion (last visited June 5, 2026).

5. When lawyers create or maintain these tools, the question arises whether the lawyers are assisting another, here AI-powered technology, in engaging in the unauthorized practice of law. Similarly, such technology is unlikely able to exercise the independent professional judgment and provide the nonlegal counseling needed in many legal situations. See ABA and Virginia Rules 2.1.

> ABA Model Rule 2.1: Advisor
> In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.
>
> Virginia Rule 2.1. Advisor
> In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

E. Communication

1. Another ethical issue concerns lawyers' duty to keep their clients "reasonably informed" about their matters and to "reasonably consult with the client about the means by which the client's objectives are to be accomplished." See ABA Model Rule 1.4.

> ABA Model Rule 1.4: Communications
> (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.

2. From this duty, the question arises whether lawyers must consult with their clients when they use AI, particularly generative AI, to conduct the tasks needed to represent the client. Lawyers, of course, do not generally need to consult with

their clients when they use technology to assist in the representation, as such assistance should reasonably be assumed. As potential uses for technology expand, however, and take on (as noted above) tasks traditional performed by humans, such delegation to AI resembles outsourcing client work to nonlawyers. Such outsourcing may require client consent.

3. According to the New York State Bar Association Report on AI (cited below), "The California bar association recommends that lawyers inform their clients if generative AI tools will be used as part of their representation. The Florida bar association takes its recommendation a step further, suggesting that lawyers obtain informed consent before utilizing such tools." (Report at page 35). See also 2007 North Carolina Ethics Op. 12 (adopted April 25, 2008) (allows such outsourcing "provided the lawyer properly selects and supervises the foreign assistants, ensures the preservation of client confidences, avoids conflicts of interests, discloses the outsourcing, and obtains the client's advanced informed consent").

4. Moreover, if the lawyers' use of AI materially impacts the lawyers' fee, the general allocation of authority between clients and lawyers supports discussing these impacts with the client. See ABA Model Rule 1.2.

> ABA Model Rule 1.2: Scope of Representation and Allocation of Authority Between Client & Lawyer
> (a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.
> (b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.
> (c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.
> (d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.
> *Comment*
> [2] On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. *Conversely, lawyers usually defer to the client regarding such questions as*

the expense to be incurred and concern for third persons who might be adversely affected. (emphasis added)

F. Fees and Billing

1. Lawyers have a general duty to ensure their fees are "not unreasonable." See ABA Model Rule 1.5(a) (note that certain states ethics rules have slightly different standards regarding fees). With the ability of AI to enable lawyers to complete certain legal tasks much more quickly, lawyers must ensure their fees remain ethically compliant. Lawyers who bill hourly therefore cannot charge for time they would have spent on a matter but no longer need to because of their use of AI. Of course, lawyers remain free to charge clients through other methods, such as flat fees, as long as the fee remains "not unreasonable" and does not mispresent the time the lawyer spent on the matter.
2. In addition to their base fee, lawyers generally may not charge clients an overhead or administrative fee in which they roll in the firm's general expenses for office-related costs, which could include costs associated with technology (like AI). Although decided well before the advent of AI technology in lawyering, a 1993 ABA Formal Ethics Opinion includes reasoning that clearly applies to billing for lawyers' use of such technology. Specifically, the opinion reasoned that lawyers cannot charge clients general office overhead absent disclosure to the client in advance of the engagement. The opinion also prohibits surcharges on expense disbursements above the amount actually incurred in directly representing the client, absent disclosure to the client.
3. From this reasoning, lawyers who seek to pass along AI costs to their clients must not do so through a general administrative fee, unless they disclose this fee to the client prior to the engagement. Similarly, absent client consent, they cannot directly bill clients for AI services over the amount those services cost the lawyer for the specific work the lawyer dedicates to the client. See also 2022 North Carolina Formal Ethics Opinion 4 (adopted October 27, 2023) (addressing billing of expenses to clients).

VI. Specific Risks of Generative AI: Hallucinations and Model Biases

a. "Hallucinations" refer to instances where the AI model generates text that is incorrect, nonsensical, or fabricated. These hallucinations can manifest as factual inaccuracies, invented information, or illogical statements that seem plausible but are ultimately false.
b. In his 2023 Year-End Report on the Federal Judiciary, Chief Justice John Roberts said "[A]ny use of AI requires caution and humility. One of AI's prominent applications made headlines this year for a shortcoming known as 'hallucination,' which caused the lawyers using the application to submit briefs with citations to non-existent cases. (Always a bad idea.)"
c. Examples of Hallucinations
    i. Fabricated Facts—The model might generate detailed but entirely invented historical events, scientific findings, or personal anecdotes that sound plausible but are false.
    ii. Misattributions—GPT might attribute quotes, works, or ideas to the wrong authors or sources, creating a false narrative.

iii. Logical Inconsistencies—The model can produce text that contradicts itself within a single response, indicating a lack of coherent understanding.

d. Hallucinations can occur for several reasons.
    i. Training Data Limitations—GPT models are trained on vast datasets collected from the internet, which contain a mixture of accurate and inaccurate information. During training, the model learns patterns and associations from this data, but it does not have an intrinsic understanding of truth or context. As a result, it can generate plausible-sounding but incorrect information based on patterns in the training data.
    ii. Pattern Recognition Without Understanding—GPT models operate by recognizing and reproducing patterns in text. They do not have a true understanding of the content they generate. This lack of understanding can lead to situations where the model produces text that follows linguistic patterns but lacks factual accuracy.
    iii. Lack of Real-World Knowledge—While GPT models have access to a wide range of information, their knowledge is static and limited to what was available in the training data up to a certain cutoff date. They do not have the ability to access real-time information or verify facts dynamically. This limitation can result in outdated or incorrect responses.
    iv. Inference from Insufficient Context—GPT models generate responses based on the immediate context provided in the input text. If the input is vague, ambiguous, or lacks sufficient context, the model may fill in gaps by generating plausible but incorrect information. This is particularly common when the model attempts to provide detailed answers with limited input.
    v. Biases in Training Data—The data used to train GPT models can contain biases, inaccuracies, and fictional content. These biases can influence the model's outputs, leading to the generation of hallucinated information that reflects the underlying biases or errors in the training data.
    vi. Probabilistic Nature of Generation—GPT models generate text based on probabilities. They predict the next word in a sequence based on the likelihood derived from the training data. While this probabilistic approach enables the generation of coherent text, it also means that the model can sometimes produce incorrect or nonsensical outputs if the probabilistic cues lead in that direction.

e. Mitigating Hallucinations—To mitigate the occurrence of hallucinations, several strategies can be employed. Some strategies can be employed by lawyers themselves whereas others depend on the AI models they select to use. Lawyers therefore can research to determine whether the models they use employ RAG, for instance.
    i. Post-Processing Verification—Implementing mechanisms to verify the accuracy of the generated content post-generation can help catch and correct hallucinations. This might involve human oversight or automated fact-checking tools.
    ii. Improving Training Data—Enhancing the quality and accuracy of the training data can reduce the likelihood of hallucinations. This includes curating datasets that are more reliable and less biased.

iii. Contextual Prompts—Providing clearer and more specific input prompts can help the model generate more accurate and contextually appropriate responses.
iv. Feedback Loops—Incorporating feedback from users and real-world use cases can help improve the model's performance over time, allowing it to learn from mistakes and reduce hallucinations.
v. Hybrid Models—Combining GPT models with other systems that have access to real-time information or domain-specific knowledge can improve the overall reliability of the responses.
vi. Retrieval-Augmented Generation (RAG)—RAG "is an AI framework for improving the quality of LLM-generated responses by grounding the model on external sources of knowledge to supplement the LLM's internal representation of information. Implementing RAG in an LLM-based question answering system has two main benefits. It ensures that the model has access to the most current, reliable facts, and that users have access to the model's sources, ensuring that its claims can be checked for accuracy and ultimately trusted." *What is retrieval-augmented generation?* https://research.ibm.com/blog/retrieval-augmented-generation-RAG (August 22, 2023) (last visited June 5, 2026).

f. Examples/Case Summaries of Lawyers' Misuse of AI—Unfortunately, these cases continue to grow in number and frequency. One database reported that in the three-year period ending April 2026, 1035 judicial decisions referenced confirmed or alleged AI hallucinated errors. (AI Hallucination Cases Database – Damien Charlotin). Here are some examples:

i. *In re Prince Global Holdings Limited, et al., No. 26-10769* (April 18, 2026)—Letter from Sullivan & Cromwell acknowledging AI-research hallucinations resulted in "inaccurate citations and other errors" in bankruptcy proceedings. The errors took three single space pages to list.
ii. *Mata v. Avianca, Inc.*, 22-cv-1461 (PKC) (S.D.N.Y. June 22, 2023)—In this case, two lawyers were fined $5,000 for submitting a brief that included fictitious legal research generated by ChatGPT. The judge in the case ruled that the lawyers acted in bad faith by relying on the AI-generated research without verifying its accuracy. *See* https://www.mindingyourbusinesslitigation.com/2023/06/artificially-unintelligent-attorneys-sanctioned-for-misuse-of-chatgpt/
iii. *Park v. Kim*, No. 22-2057 (2d. Cir. January 30, 2024)—The United States Court of Appeals for the Second Circuit referred a New York lawyer to its Grievance Panel for potential disciplinary action after using ChatGPT to research prior cases for a medical malpractice lawsuit and citing a non-existent state court decision. *See* https://caselaw.findlaw.com/court/us-2nd-circuit/115760381.html.
iv. Michael Cohen's Lawyer—On March 20, 2024, a federal judge in New York declined to sanction Michael Cohen and his lawyer David Schwartz for submitting fake case citations generated by Google's Gemini (formerly known as Bard). The judge called Schwartz's conduct "certainly negligent, perhaps even grossly negligent," but he found no evidence of bad faith to warrant

sanctions. *See* https://www.reuters.com/legal/michael-cohen-wont-face-sanctions-after-generating-fake-cases-with-ai-2024-03-20/.

v. *People v. Zachariah C. Crabill*. 23PDJ067. November 22, 2023—In May 2023, Crabill filed a motion that included fictitious case law generated by ChatGPT. He failed to verify the information before submission and initially blamed an intern for the error when questioned by the judge. The Colorado Supreme Court suspended Crabill for a year and a day, including a 90-day suspension and a two-year probation period. *See* https://coloradosupremecourt.com/PDJ/Decisions/Crabill,%20Stipulation%20to%20Discipline,%2023PDJ067,%2011-22-23.pdf.

g. New York State Bar Association Report on Artificial Intelligence

i. On April 6, 2024, the New York State Bar Association issued a 92-page report titled "Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence." *See* https://nysba.org/app/uploads/2022/03/2024-April-Report-and-Recommendations-of-the-Task-Force-on-Artificial-Intelligence.pdf. The Executive Summary provides: "Artificial intelligence, particularly generative AI, has had a profound impact across multiple sectors of our society, revolutionizing how we approach creativity, problem-solving and automation. From art and entertainment to healthcare and education, AI is reshaping industries, creativity and society in multifaceted ways. While AI and generative AI offer immense potential for innovation and efficiency, the technology also presents challenges that require careful management, including ethical considerations, privacy concerns and labor impact. The ongoing evolution of generative AI promises to continue influencing the world in unprecedented ways…. Here, we summarize our four principal recommendations for adoption by NYSBA.

1. Adopt Guidelines: The Task Force recommends that NYSBA adopt the AI/Generative AI guidelines outlined in this report and commission a standing section or committee to oversee periodic updates to those guidelines.
2. Focus on Education: The Task Force recommends that NYSBA prioritize education in addition to legislation, focusing on educating judges, lawyers, law students and regulators to understand the technology so that they can apply existing law to regulate it.
3. Identify Risks for New Regulation: Legislatures and regulators should identify risks associated with the technology that are not addressed by existing laws, which will likely involve extensive hearings and studies involving experts in AI, and as needed, adopt regulations and legislation to address those risks.
4. Examine the Function of the Law in AI Governance: The rapid advancement of AI prompts us to examine the function of the law as a governance tool. Some of the key functions of the law in the AI context are: (i) expressing social values and reinforcing fundamental principles; (ii) protecting against risks to such values and principles;

and (iii) stabilizing society and increasing legal certainty is included in the Appendix."

APPENDIX TO SECTION 1
New York State Bar Association Warns That AI Must Not Compromise Attorney-Client Privilege

By David Alexander
April 8, 2024

https://nysba.org/new-york-state-bar-association-warns-that-ai-must-not-compromise-attorney-client-privilege/

The New York State Bar Association is advising lawyers to ensure that artificial Intelligence does not put attorney-client privilege at risk at a time of increasing security concerns about confidential information being disclosed by the technology.

The report from the association's Task Force on Artificial Intelligence, which was approved by its governing body, the House of Delegates, on Saturday, advises lawyers to disclose to clients when AI tools are employed in their cases. Under the Rules of Professional Conduct, attorneys also have an obligation to make sure that paralegals and other employees are handling AI properly, the report states.

The task force determined that New York's Rules of Professional Conduct provide helpful guidance governing attorneys' use of AI but said that more education was needed to make sure that attorneys and judges are handling the technology properly. The report also says that legislation may become necessary to govern its use.

"AI can enhance the delivery of legal services. It obviously has enormous potential because it can already draft documents, conduct research, predict outcomes, and help with case management. However, we have an obligation as attorneys to be aware of the potential consequences from its misuse that can endanger privacy and attorney-client privilege," said Richard Lewis, president of the New York State Bar Association. "I thank the task force for addressing this complex matter and providing direction on how we can incorporate it into our daily routines in a safe manner."

The report also recommends that the association form a standing committee to address evolving AI issues including ethical concerns that derive from the technology's tendency to hallucinate. The most serious hallucinations have resulted in citations and quotes from non-existent cases being included in briefs.

"Artificial Intelligence is the latest technological evolution that at one moment awes us and the next fills us with anxiety," said Vivian Wesson, chair of the task force and executive vice president and general counsel at The Board of Pensions of the Presbyterian Church. "We are aware of the enormous impact it will have on our profession but are also familiar with the many risks it poses

regarding confidentiality. The technology is advancing at an alarming rate and so it is imperative that we address it at this time."

Other recommendations include:

- Legislators should determine whether AI regulations should be applied in a one-size-fits-all approach or through industry-specific regulation.
- Attorneys should consider whether the use of AI will help them represent their clients more effectively before employing it.
- In addition, the New York State court system's Appellate Division should consider rewriting the Rules of Professional Conduct to make it clear that attorneys should:
    - Have the latest information on technology (including AI and GenAI) that improves the quality of legal services.
    - Determine whether the use of AI enhances legal services on a case-by-case basis.
    - Be competent about how AI tools operate to better ensure that the research generated is legitimate.

Christian Legal Society National Conference
Denver, Colorado, October 9, 2026

AI, DEMOCRACY, AND THE RULE OF LAW

SECTION 2: Considerations Regarding AI, Inalienable Rights, and Governance

1. **Overview and AI Level-setting: Five Key Characteristics of AI, and why they matter to democracy, the rule of law, and human dignity:**

    a. **AI as a General Technology**. AI – an "omni-use technology" – is impacting virtually every sector of the economy and civic endeavor, and diffusing at unprecedented pace and scale. Corollaries to this acceleration of technological progress and opportunity are the practical, ethical, and moral risks which are difficult to assess and manage. Society and government institutions face rapidly iterating disruptions in areas including biotech, defense and national security, financial and labor markets, and education. At the personal level, which impacts the capacity of citizens to responsibly engage in self-governance, the diffusion and ubiquitous reliance on AI applications also may significantly impacts how we gather, assess, and assign confidence to information we receive, and how we exercise judgment about the extent to which we should rely on AI products we consume.

    b. **Agentic AI:** <u>For the first time in history</u>, we have developed, released, and increasingly may delegate agency to non-human mechanisms, which we may come to rely on to manage critical tasks. These AI agents may be able to create successive generations of AI agents, limited only by energy and computing power constraints and by the extent that humans can, and do, effectively "align" AI with human-instantiated goals, values and operational parameters.
        i. How do these agents, and our reliance on them, promote or undermine human agency, dignity, flourishing, and democracy?
        ii. How does recognition or denial of legal status of AI agents mitigate for or against the value of persons in society?

    c. **AI is not a monolith**: AI development and application is not monolithic: it is widely and rapidly diffused and iterated. This diffusion challenges "alignment" policies as well as legal and regulatory parameters adopted to manage unacceptable risks or promote moral and ethical values – assuming those values can be agreed upon.
        i. To what extent does this diffusion of AI capacity align with societal mores or create externalities.
        ii. To what extent does extensive AI diffusion invite or encourage expanded government oversight capacity, and to what extent would that expanded capacity be consistent with a flourishing, free society?

    d. **Democratized AI, and the "Democratization Paradox**." Low barriers to entry for use of powerful AI and deployment of AI agents place applications of AI at the ready disposal of vastly diffuse users, creating unprecedented opportunity for innovation. As a corollary, this diffusion raises asymmetric "dual-use" risks by negligent or intentional

actors on a scale that has not been addressed by governments, regulatory agencies and even nations.[4] Real or imagined response to risks can create a "democratization paradox,"[5] encouraging or inviting expansion of government control and oversight on scales not previously experienced.[6]

e. **AI as non-human intelligence**. For the first time in history, other than in the spiritual realm, humans will interact with, respond to, and increasingly rely on a non-human intelligence mechanism that at least in some respects (e.g., computation capacity and the access to all knowledge domains at once) exceeds human capacity.
   i. What legal rights may or should be assigned to AI models and agents, and what are the implications for respect for human rights and dignity of assigning such rights?
   ii. How will access to and reliance on AI-generated information and analysis impact human capacity to obtain and discern information essential to informed citizen participation in society?
   iii. What moral parameters may be adopted by these diffuse AI agents, and how will society come to adopt these results as normative?

---

[4] *See, e.g.*, Dario Amodei — Policy on the AI Exponential, June 2026: "In the last few months… the evidence of AI's incredible power, as well as its risks, has become undeniable. Perhaps the most emblematic example is Claude Mythos Preview and the discovery that frontier models pose very real risks to cybersecurity, creating the potential for disruption of the financial sector, critical infrastructure, and national security. Mythos Preview scrambled the global cybersecurity landscape. But ***its broader significance is that it proves beyond doubt that AI models are now tools of global and national strategic consequence. The cyber risks that Mythos-class models present will not be the last that we must face. I believe that biological risks may soon follow, and that serious AI autonomy risks may not be far behind.***" (*Emphasis added.)*

[5] As used here, the "democratization paradox" describes a potential response to significant negative risks (e.g., mutated virus or other biotech accident, bioterrorism, threats to energy grids, financial infrastructure or other national security risks) which are propagated and harder to detect and pre-empt due to "democratized" diffusion of AI technologies, and which result in pressure to expand government surveillance, enforcement and police power to protect against and mitigate the harms these risks may cause.

[6] *Op.cit.*, Dario Amodei — Policy on the AI Exponential, June 2026: "**It is time to go beyond transparency to more serious and binding regulation of AI**… . I am grateful to see the Trump administration's Executive Order move incrementally towards a greater role for government in AI, though Anthropic's proposal recommends even further action. Our proposal includes the following elements:

- Models above a threshold of compute should undergo mandatory testing by a qualified third party for their level of risk in four specific areas: cybersecurity, biological weapons, loss of control of AI systems, and automated R&D that could accelerate these other risks.
- The government should have the power to block or deter deployment of the model if it is determined, in light of third-party assessment, to present unacceptable risks… .
- Third-party evaluation could be done by a government agency (similar to the FAA) or a set of private organizations that are authorized and inspected by the government to evaluate models according to certain standards (a "regulatory markets" approach).
- AI companies that develop advanced AI models must have strong security standards that protect their model weights, should conduct regular red teaming and penetration testing, and should work with the government to defend against major threat actors.
- Safety incidents in the four critical areas must be reported promptly.

There may come a time, perhaps relatively soon, when we need to go beyond this, when the most powerful AI systems look less like airplanes or automobiles and more like weaponizable nuclear materials—a threat to humanity rather than "just" a threat to public safety. If that occurs, we may need more aggressive regulatory measures than those I have laid out. But…I don't think we should get ahead of ourselves." (*Emphasis added.)*

iv. How does reliance and affirmation of AI intelligence strengthen or undermine respect for human dignity, and for the inalienable rights which are premised on this understanding of human dignity?

2. **AI and Inalienable Rights:** AI pressures the balancing of key constitutional rights. How should government policy protect national interests, while also respecting fundamental constitutional values?

   a. AI, Government Surveillance, and the Fourth Amendment:

   i. Challenge to Fourth Amendment values, arising from the promise of enhanced security. Larry Ellison, Oracle founder and Executive Chairman, reported on the company's prospects using AI-fueled tech: "Most of the world's important data is in an Oracle database… .The police will be on their best behavior because we will be constantly watching and recording everything that going on. Citizens will be on their best behavior, because we'll be constantly recording and reporting everything that's going on. It's unimpeachable… . We can use AI to monitor the video." Financial Analyst Meeting 2024 | Oracle, September 12, 2024.

   ii. Legal precedent remains unsettled regarding government ability, without a warrant, to access citizen (and non-citizen) records that are captured by private interests and third parties.

      1. *See., e.g., Carpenter v. United States, 585 U.S. 296 (2018),* (refraining from ruling that the Fourth Amendment always requires the government to obtain a warrant when seeking information citizens voluntarily disclose in contracts with third parties.)
      2. Increasingly, U.S. and state law enforcement agencies acquire AI-synthesized information from private sources, whether by administrative warrant or outright data purchases from private sources trading in personal data.
         a. DHS spent a record $425 million on surveillance tech in the past year [2025], a 17% increase from the prior year. Federal spending is on pace to set another record in 2026, according to an analysis of federal contract data by the Journal. This newly expanded domestic surveillance system allows thousands of federal agents nationwide to peruse a trove of data belonging to more than 300 million people, including citizens.' We Know You Live Right Here': No Secrets in America's New Surveillance Dragnet - WSJ.

   b. AI and the First Amendment.

   i. On what basis should we accord First Amendment protections to AI chatbots and other sources? To the extent proponents would extend such rights to these novel entities, what does this do to our respects for, and understanding of, the value of human dignity and personhood? See Ryan Bangert and James Tedesco, *The Ghosts in the Machine: How Generative AI Will Test the Bounds of the First Amendment,* 29 TROLP 3, Feb. 7, 2026, at THE GHOST IN THE MACHINE: HOW GENERATIVE AI WILL TEST THE BOUNDS OF THE FIRST AMENDMENT — TROLP.

ii. **Executive branch uses of AI to accomplish government priorities, and the potential abuse of those powers to convey government- approved messages.** The line between ensuring that government can communicate its policy messages to citizens while not using its power to improperly constrain or compel messages that challenge the government's viewpoint, is difficult to draw and fraught with potential for abuse of First Amendment rights. The stakes for who controls these messages and how government exercises its ability to influence which messages are amplified and which are restricted are central to democracy. One case study is the *Missouri v. Biden* saga:

1. See, e.g., *Missouri v. Biden*, 680 F.Supp.3d 630 (W.D. La. 2023), found that U.S. Government actors likely had caused certain plaintiffs to be deplatformed by major social media companies. Exertion of executive branch pressure on social media and ISP providers, to deplatform contrary and unwelcome messages about COVID, etc.
2. The Fifth Circuit, *State of Missouri v. Biden,* 83 F.4th 350 (2023) modified the lower court injunction prohibiting specific government actors from attempting to coerce or significantly encourage social media platforms' content-moderation decisions; and determined that the government's actions, such as issuing intimidating messages, effectively commandeered the platforms' decision-making processes, and rendered the private companies' moderation choices a form of government action, subject to First Amendment limitations.
3. In 6-3 decision, *Murthy v. Missouri, 603 U.S. 43 (2024),* the Supreme Court reversed the Fifth Circuit, ruling plaintiffs lacked standing because they failed to establish a direct, traceable link between the government's communications and removal of the posts (rather than the platforms' independent enforcement of their own policies).
4. Trump administration issues Executive Order, Restoring Freedom Of Speech And Ending Federal Censorship – The White House, 90 Fed. Reg. 8243 (Jan. 28, 2025), responding to alleged White House exertion of coercive pressure on third parties, such as social media companies, to moderate, deplatform, or otherwise suppress speech that the Federal Government did not approve.
5. March 2026, The U.S. Justice Department entered into a consent decree with Louisiana and Missouri, permanently enjoining the U.S. Surgeon General, the CDC and the Cybersecurity and Infrastructure Security Agency from coercing social media companies to remove content. Missouri v. Biden, (consent decree at Civil Action No. 22-cv-1213, March 24, 2026, @ gov.uscourts.lawd.189520.477.1.pdf).[7]

[7] "The Parties … agree that government, politicians, media, academics, or anyone else applying labels such as "misinformation," "disinformation," or "malinformation" to speech does not render it constitutionally unprotected. *See United States v. Alvarez* (2012) (plurality op.) … [T]he Government [therefore] cannot take actions, formal or informal, directly or indirectly—except as authorized by law—to threaten Social-Media Companies with some form of punishment (i.e., an adverse legal, regulatory, or economic government sanction) unless they remove, delete, suppress, or reduce, including through altering their algorithms, posted social-media content containing protected free speech…".

"The Surgeon General, the Centers for Disease Control and Prevention (CDC), the Cybersecurity and Infrastructure Security Agency (CISA) ("Enjoined Defendants"), and their employees and agents, shall take no actions,

c. **AI and Access to Justice**:
    i. Will *pro se* litigants be able to use AI to expand their access to courts and the vindication of their rights, and will whatever advantage they obtain be equal to the advantage and efficiencies that law firms will capture from their routine, sophisticated use of AI tools?
    ii. How will the courts respond to anticipated increase in volume of AI-generated massive complaints? See, e.g.:
        1. Artificial Intelligence Floods Court Dockets with Home-Brewed Lawsuits - The New York Times, Mattathias Schwartz and Zach Montague, May 25, 2026.
        2. Why lawyers keep citing fake cases invented by AI | Scientific American, Stephen Melendez, May 22, 2026.

3. AI Pressures on the Rule of Law.

a. AI and Executive Power consolidation of power in response to national security and economic priorities: How and to what extent should government manage AI risk/opportunity implications while protecting US national security and economic interests, without stifling innovation?

i. **Federalism and Preemption of State Action on AI:**
    1. Federal efforts to encourage AI development and preempt patchwork of state regulation:
        a. Trump Administration Executive Order, *Ensuring a National Policy Framework for Artificial Intelligence* (Dec. 11, 2025), announces initiative through federal agency action and litigation targeting state laws for preemption under the Constitution, existing federal legislation, and future legislation. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
        b. *x.AI LLC v. Weiser*, Civil Action No. 1:26-cv-01515, U.S. District Court for the District of Colorado. Elon Musk/x.AI sues to block Colorado AI regulation, which requires "high-risk" AI developers to exercise reasonable care to protect consumers from "algorithmic discrimination."
            i. USDOJ intervenes in the suit, alleging "…the Colorado law violates the Equal Protection Clause of the Fourteenth Amendment by requiring AI companies to prevent unintentional disparate impact that their products could have based on protected characteristics

---

formal or informal, directly or indirectly—*except as authorized by the Constitution, statute, judicial order, or regulation*—to threaten Social-Media Companies with some form of punishment (i.e., an adverse legal, regulatory, or economic government sanction) unless they remove, delete, suppress, or reduce, including through altering their algorithms, posted social-media content containing protected free speech. Nor shall Enjoined Defendants unilaterally direct or veto social media content moderation decisions of Social Media Companies." *(Emphasis added).*

like race and sex, and by exempting liability for certain forms of discrimination designed to advance 'diversity.'" Office of Public Affairs | Justice Department Intervenes in xAI lawsuit Challenging Colorado's 'Algorithmic Discrimination' Law | United States Department of Justice .

2. **Numerous and diverse state attempts to regulate across a wide range of areas, including, safety, surveillance, privacy, elections,** intellectual property, and denying "personhood" status to AI:
    a. See, e.g., extensive state efforts:
        i. California:
            1. AB-2655 Defending Democracy from Deepfake Deception Act of 2024, Bill Text: CA AB2655 | 2023-2024 | Regular Session | Enrolled | LegiScan
            2. California Transparency in Frontier Artificial Int elligence Act (TFAIA) , SB 53, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53
            3. See
        ii. Utah Artificial Intelligence Consumer Protection Amendments, SB0226.
        iii. Tennessee Ensuring Likeness, Voice, and Image Security Act of 2024
    b. See also Smith, Austin et al., *Denying Personhood to AI: An Analysis of U.S. State Legislation on AI Legal Status (May 25, 2026). Available at SSRN: https://ssrn.com/abstract=6829981*

ii. **Continuing AI developments cause U.S. Administration to consider a more active regulatory approach with respect to national and economic security concerns triggered by AI releases.** Case study: Anthropic release of Claude Mythos and subsequent products:
    1. April 2026. Anthropic announces Claude/Mythos, designed to discover software bugs and vulnerabilities, but recognizes its power and potential for misuse (creating a roadmap of vulnerability for hackers), and thus restricts its availability to limited AI providers and government. Anthropic cooperates with White House to avoid potential harmful misuse. White House and Anthropic urgently brief Federal Reserve bank and other financial institutions on potential threats from Mythos misuse.
    2. Late April 2026: Anthropic proposes Mythos release to somewhat wider array of companies to "harden" computer systems and applications, but White House resists this wider release, on security grounds. Anthropic acquiesces for the time being.
    3. June 2, 2026: After issuing and pulling back an executive order in May, White House issues executive order, Promoting Advanced Artificial Intelligence Innovation and Security – The White House. EO calls for

extensive executive branch assessment of security risks at every relevant agency within 30 days, but **adopts a voluntary compliance approach** for industry: "Nothing in this section shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models."

4. June 5, 2026: Anthropic announced intent to release Fabel 5 ("slimmed down" version of Mythos 5, meant for more widescale public use). But on June 12 the **US restricted Fabel 5 and Mythos 5 from export to foreign governments, companies and individuals**. See, Anthropic Halts Access to Top AI Models After U.S. Ban on Foreign Use - WSJ