AI
At the Crossroads of Law and Healthcare
- RADIC Presentation

Peter Kelman, Esq.
www.kelmanlaw.com
pkelman@kelmanlaw.com

500 Unicorn Park Drive, Suite 300
(508) 314- 0943

Table of Contents

Intro – Who am I

- I was programming computers before most of you were born
- Dave was my instructor many decades ago. He taught me Lotus (remember them?) Notes
- I represent software companies and entrepreneurs in litigation and in transactions such as licensing arrangements and entity creation
- Because I understand technology, I find the underbelly of software companies, for example:
- I sued eBay, and while I am prohibited from saying my client won, I can say my client left very happy
- Author of articles about technology and the law published by: *The American Bar Association, Massachusetts Lawyer's Weekly, The Boston Business Journal, Mass High Tech*

Sources of Influence

- Ethical
- Legal
  - Regulatory (i.e. statutes and regulations)
  - Non-regulatory (private causes of action)
- Medical

What is AI?

- Perhaps, nothing new?
  - *See* Appendix A, my article, "*The Rise of Natural Stupidity*"
  - I must have known I would be giving this talk when I wrote that two years ago, because it is all about the medical pun at the end of the article

- AI and Machine Learning ("ML") often used interchangeably, but really different software implementations

What is AI?

- Here's how Congress defines AI:

  The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action. - 15 USC § 9401(3)

- The European Union ("EU") defines AI "system" as:

  'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

- **Under these definitions, is a device that counts cards in Las Vegas an AI system**?

- **Is the Turing Test definition of AI the opposite of the definition Supreme Court Justice Potter Stewart gave to pornography: "I know it when I see it"?**

Regulatory Environment – U.S.

- Laws, in the form of statutes and regulations, govern our behaviors
- In general, federal law trumps state law (pun intended)
- Federal Regulatory Environment of AI:
  - It doesn't exist
  - Executive Order 14179, 1/23/25, "Removing Barriers to American Leadership in Artificial Intelligence", Appendix B
  - Executive Order of 12/11/25, "Ensuring a National Policy Framework for Artificial Intelligence", Appendix C

Regulatory Environment – U.S.

- State laws, in the absence of federal law, can regulate business (nature abhors a vacuum)
- *See* Appendix D, a list of state legislation regulating the use of AI in healthcare
- Currently 13 states have passed healthcare AI laws
- What is a company to do with such a patchwork of regulations?
  - Pray?
  - Pay?
  - Conform to California?
  - Target certain states?
  - Obey the EU? (segue into next slide)

Regulatory Environment – E.U.

- E.U. is the yin to the U.S. yang of AI regulation
- In 2016, EU passed the General Data Protection Regulation ("GDPR")
  - Intended to protect the privacy rights of individuals from abuse in computer systems and over computer networks
  - De facto standard for privacy that many software companies observe, even those not in the E.U., but applicable any company that does business in the E.U.
- Article 22 of the GDPR presaged the current A.I. environment

Regulatory Environment – E.U.

- Article 22 of GDPR states in part:
  - The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- Full text of Article 22 is Appendix E
- Recent court decisions in the E.U. have held that AI systems are regulated by Article 22 and subject to its requirements and prohibitions. *See* Appendix F.

Regulatory Environment – E.U.

- In 2024, EU passed the Artificial Intelligence Act
- While Washington takes a laissez-faire approach to AI regulation, the EU is tackling it head on
- Many provisions of the AI Act do not take effect until later in 2026
- In general, the AI Act regulates AI systems in proportion to how life-critical those systems are, or the degree of risk involved in the application
- In other words, health care companies are directly in the cross-hairs of extensive AI regulation by the EU
- Appendix G is a brief article describing the impact of the AI Act on health care companies

Regulatory Environment – E.U.

- Some of the key parameters regulated by the AI Act for high-risk applications are:
  - The involvement of a human being before final decisions are communicated to end-users
  - Be subject to continuous quality control supervision
  - Inform end-users of the use of AI in the decision making process
- Appendix H is a brief list of requirements imposed on high-risk applications by the AI Act

Non-AI Specific Regulations

- While U.S. does not have federal regulations targeting AI, AI is subject to other health care regulations, such as:
- HIPAA (Health Insurance Portability and Accountability Act)
  - Confidentiality concerns
  - Disclosure concerns
  - Consent concerns
- *See* Appendix I, *"When AI Technology and HIPAA Collide"*

Regulatory Wrap - Up

- Federal AI regulations do not exist, but AI subject to HIPAA
- Until such time as they may be superseded by future federal regulations, state laws govern AI applications in the U.S.
- The EU regulatory environment is dynamic and U.S. companies are well-advised to comply with provisions of the GDPR and AI Act

Non-Regulatory AI Issues

- “AI” is embedded in the word “plaintiff”
- Individuals (and companies) have rights created by legal doctrines even if those rights are not codified by statutes
- Generally an actor, whether a person or a company, is liable to a third party if the actions of the actor cause harm to the third party.
- This is called a tort

Primer on Tort Law

- A Plaintiff can sue a defendant when no contract exists between plaintiff and defendant, if plaintiff can prove:
  - Defendant owed a duty to plaintiff;
  - Defendant breached that duty; and
  - Defendant's breach of duty caused harm to Plaintiff
- This is called negligence

Potential Tort Liability Created by AI

- A company is responsible for what it says and does
- If a system's output is relied upon by a user and the user is injured, the company may be liable in tort to the injured party
- Typical tort actions include malpractice, defamation, invasion of privacy
- *See* Appendix J, part IV about Mark Walters, an article I wrote about defamatory liability of AI output.

How to Limit Tort Liability

- DISCLAIM, DISCLAIM, DISCLAIM!!!
- INFORM, INFORM, INFORM!!!
- Require end-users to acknowledge they have been informed about the use of AI in the output they receive
- Give users the ability to opt-out of further interaction with an AI based system
- Best antidote to process-based negligence:
  - Operate consistent with the standard of care in your industry
  - i.e. keep up with the joneses; do as your neighbor does
  - E.g. for RADIC, identify your peers (perhaps CHAI, Mayo Clinic) and adopt practices and procedures similar to theirs

How Other Organizations are Monitoring the Use of AI

- The American Bar Association has issued a formal opinion on the use of AI by lawyers.
- Some items discussed in the opinion are:
  - Privacy concerns that confidential information does not enter the public domain by ingestion by a large language model
  - Accuracy concerns, that the lawyer does not mistake an ai hallucination for a real-life event
  - Preparation concerns, that lawyers don't let the output of AI substitute for their own preparation
- *See* Appendix K.

Intellectual Property Rights and AI

- AI has created intellectual property issues concerning:
  - Input to AI
  - Output from AI
- Input Issues:
  - Do AI companies violate the rights of authors whose works are used in large language and image models?
  - Authors and institutions such as the NY Times, say “yes”
  - I say “no”, see Appendix J, parts 1 – 3, about copyright law and AI
  - Courts are still deciding, the weight of authority indicates “no”
- Output Issues:
  - Does the output of generative AI create a protectible property interest?
  - Yes, which is owned by the user, not by the computer
  - The U.S. copyright office has denied an application for copyright filed on behalf of a computer; but the owner of the computer could file for copyright protection

Conclusion – How does this Compare to the AI Version of this Talk

- One can not conclude a talk on AI and Healthcare without having asked an AI language model to prepare the same presentation.
- Appendix L is the presentation AI thought I should deliver.
- Which do you like better?

Conclusion – Why ChatGPT says we should Believe it

- I asked ChatGPT why we should believe what it says about AI and Healthcare laws
- Appendix M is its answer
- IMHO, its answer presents a nutshell of the strengths and weaknesses of the content of Generative AI:
  - Strengths: smarmy, superficially ingratiating, almost nearly accurate, conversationally appropriate, but dull
  - Weaknesses: content is hugely incomplete, it missed talking about the AI Act and omitted any reference to state law
  - Result: if it were a lawyer, it would be sued for malpractice
  - **Caveat Emptor!!**

Thank you!

Peter Kelman, Esq.
www.kelmanlaw.com
pkelman@kelmanlaw.com

500 Unicorn Park Drive, Suite 300
(508) 314- 0943

Index to Appendix Articles

Appendix A

The Rise of Natural Stupidity

- ***As published in the Boston Business Journal, April 24, 2025***

I. Introduction

It's a tale as old as time. Every movement gives birth to a counter-movement. Newton codified it as his third law: For every action there is an equal and opposite reaction. While Newton was describing the characteristics of material objects and laws of physics, his observation holds true for social as well as physical movement. Every strongly-held belief seems to engender the creation of an opposite belief. Another way to put it is that for every Superman there is a Lex Luthor. Religious worshippers butt heads with atheists; Republicans with Democrats; Yankee fans with Red Sox fans; the list is endless. Now as we embark on the age of Artificial Intelligence ("AI"), we are witnessing the rise of its counter-movement, its nemisis: Natural Stupidity ("NS").

It is always exciting to believe you are witnessing the birth of something. Certainly that seems to be the prevailing sentiment about AI. That somehow AI is heralding a new era of computer processing; its output is unlike anything computers have produced before. Which message appears deeply unsettling to many people. Most of those unsettled by AI warn of the negative consequences of its deployment. They advocate limits on AI

applications. They want to restrict the output of AI, prevent it from creating digital images, from creating text documents. There are some who call for certain AI to be illegal; the United States federal government has resisted passing legislation to regulate AI. Instead Presidential guidelines have been promulgated to help guide AI developers. These guidelines are in the form of an executive order; as such they do not have the power of a legislatively passed statute. One could say these guidelines are "aspirational" objectives that AI developers should aspire to adhere to but are not required to abide by.

It is fair to say that the preponderance of voices urging caution about AI are the voices of people with experience. Enough experience to know that what they now experience with AI is different from what they experienced before the advent of AI. It is the difference that troubles them. The less pre-AI experience you have, the less you are troubled by emerging AI technologies. Teen-agers are not troubled by AI; adults are. Adults caution against rapid deployment of AI applications; teen-agers are for full-throttle deployment.

This cautionary attitude regarding the deployment of AI is the hallmark of NS. Whereas AI resides solely in the architecture of computers, NS resides solely in the attitudes of human beings.

II. **Is the AI Controversy the Byproduct of an Eyeball Competition?**

Every author wants to believe that what their story is important. When was the last time you saw a headline such as, "Another Ho-Hum day in Day in Dullsville, Read about the Tedium Herein"? That does not attract eyeballs. But a title such as this, "How Nations are Losing a Global Race to Tackle AI's Harms" (*New York Times*, December 6, 2023) is meant to make you think the AI apocalypse is just around the corner, and there will be no refuge on planet earth. Or what about this title, "The Unsettling Lesson of the Open AI Mess?" (*New York Times*, November 22, 2023). It suggests that you must be a dufus not to know that there was/is an AI mess. And if you don't want to continue as a dufus, you better be sure to read this article and learn about the AI mess you may have missed. These titles self-aggrandize their authors and their publications; they desperately cry out for the attention of eyeballs. They exaggerate the importance of the topic they report on.

Which brings us to this question: is the dawn of AI, now being so thoroughly analyzed and reported on, really that important? Is it really something different from before that merits all the press it is receiving? Or is what we now read the output of some journalistic formula (perhaps the output of AI!?) designed to attract eyeballs and advertising revenue to a publication?

A fair question. If we trace the arc of computing from the abacus to today, there are many watershed moments that appear to herald breakthroughs, that appear to disrupt the

continuity of what preceded them. But have they? Just looking at the past fifty years, many technological advances have been appeared disruptive at the time of creation only to later fade into a pattern of gradual evolution. For example, the introduction of the personal computer in the 1970s and 80s took computers out of the laboratory and put them in the home. Windows transformed DOS into something more or less understood by humans. Apple transformed PCs into objects more or less understood by humans. Cell phones put the power of computers into a hand-held device, and many say have changed our world.

Is AI any more revolutionary than any of these other inventions? It would be hard to argue that what AI is doing now is more disruptive than when personal computers transformed the individual consumer into a computer operator. Or when cell phones miniaturized computers into an object that could be held in one hand while you were taking a picture with it. Can a process, a piece of software such as AI, disrupt behavior the way a physical object can?

III. **The Turing Test.**

The answer might be yes if we consider a test formulated almost 75 years ago by Alan Turing, called appropriately, the "Turing Test." Turing proposed that if a computer could produce output that was indistinguishable from the output of a person, then one could say that the computer was capable of "thought." As Turing proposed the test, if a person were to carry on a conversation between two other entities, one a person, the other a computer, and could not differentiate his conversation with the computer from his conversation with the other person, then the computer would have passed the Turing Test. In other words, according to Turing, when a computer gets so good at computing that the output of its computation is indistinguishable from the output of a human brain, then the computer can be described as "thinking."

If we believe the introduction of AI is different from the introduction of personal computing or the introduction of the cell phone, that difference might lie in this. That when we interact with a personal computer or cell phone, we know we are using a device, a gadget; we are not interacting with another person. The personal computer and cell phone each flunks the Turing Test. But when we interact with AI, we are not sure if we are reading the output of a computer or the output of a person. It appears to pass the Turing Test; the computer is "thinking" like a person. And that is unsettling. Suddenly the origin of output is up for grabs. Is the author of the output a human or a computer? No longer do we ask: to be or not to be? Now we must ask: PC or not PC?

Those who believe in NS believe if the output is from a PC and we don't know it, then civilization will come to an end before climate change causes an ambient temperature rise of 1.5 degrees Celsius. We must ask, why this fear of AI? What provides the grist that

feeds the NS mill? Is the output from AI any less reliable or more problematic than the output of humans?

IV. Never Mind if we are Talking to a Computer, Who is telling the Truth?

Let's take Turing's Test and add a second part to his test. Let's say that not only must the observer determine which if either of his communication partners is a human, he must also determine which partner he believes is telling the truth. I suspect that a believer in NS will presume the teller of truth is the human and that the computer is not to be trusted. However, I say not so fast. I believe it is just as likely, in fact even more likely than not, that the computer would be providing a more truthful answer than the person. Is that an irreverent statement?

I don't think so. I think part of what makes the Turning Test problematic, especially if we add part two to it, is that the stream of communication takes place with no context. It is a dialog happening in a vacuum devoid of non-verbal cues. Without non-verbal cues, information is lost at sea. For example, consider this hypothetical:

Let's say you are curious about Israeli – Hamas war in Gaza. You don't know much about the historical background leading up to the conflict. So you seek information from various sources. Perhaps your first instinct is to ask a friend. The friend listens to your question about the war and offers her opinion about events leading up to the war. You listen to what she says. You process her words by extracting a meaning for each of them. But at the same time, you create a context for how to interpret those meanings. For example, if you know your friend is Jewish, you might interpret her words one way. But if you know she is Palestinian, you might interpret her words a different way. What if you knew that one of her cousins had been killed in the conflict? What if you knew that one of her cousins had been captured as a hostage in the conflict? There are myriad non-verbal cues and background pieces of information that we use to filter the meaning of verbal communications. It is possible that the message we take away from a discussion with a person is vastly different from the denotative meanings of the words they used. What we remember as the content of the communication is not just the words we heard or read; it is those words filtered by the context of the non-verbal cues and background information that shape the meaning of those words.

Back to the Turing Test. If we strip away all of the non-verbal cues that provide the context to message we hear, can we believe the raw message from a person? I have my doubts. More than having doubts, I suspect the words spoken or written by a person, with no background for context, are probably less truthful than the output from AI. I suspect that an individual carrying on a conversation with two unknown sources, without any context to interpret the source of each message, would probably get a more accurate message from AI than a person.

How can we test such a hypothesis? How about looking to the ultimate spokespersons of truth in our country, our Supreme Court. We look to our Supreme Court to resolve disputes, to dispassionately interpret our laws and provide guidance developing answers grounded in the truth of our laws. In 1973, in Roe v. Wade, our Supreme Court justices told us that the truth was that our Constitution gave women the right to have an abortion. However, in 2022, in Dobbs v. Jackson different Supreme Court justices told us that the truth was that our Constitution did not give women the right to have an abortion. What is the truth of these conflicting opinions? Is there truth? Even among our most educated jurists, truth is relative. Truth is the byproduct of bias, of belief, or prejudice. It is not found in a dictionary.

V. **Bias, if Recognized, Can be Informative.**

Those who want to elevate NS over AI disregard the roles of bias and prejudice in formulating answers. Or else, without cues to recognize those biases and prejudices, they are distrustful of answers produced by AI. They can take solace in this fact: the output of AI is not without bias and prejudice. It is just that the bias and prejudice of AI cannot be detected by observing the author's skin color, age, gender, or spoken accent. However the bias and prejudice of AI is injected into the code of AI by its programmers. AI is programmed by persons who, like all persons, share certain beliefs and biases. These beliefs and biases shape the output of an AI platform.

For now, AI output it created by companies like Google, Microsoft, OpenAI, and Metadata. Companies that appear to have no political or socio-economic bias, although many consider the output of AI more representative of the views of liberal or "left-leaning" constituencies. However, It will only be a matter of time before AI technology is private labeled and offered by companies with known biases. The software companies will package their AI platforms and license them to outlets such as National Public Radio and Fox News which have well-known public personae with pre-defined political sympathies. These companies will shape the output of their AI technology platforms by feeding those platforms information supportive of their respective biases. As consumers, when we retrieve AI output from such privately label platforms with known biases, we will know how to construe the message in light of its author's context.

The proponents of NS should take comfort in the fact that the output AI is just as flawed with human bias as is the direct message from a human being. If bias floats your boat, the tides of AI are plenty high with bias. It is just that these biases are harder to detect in the output of AI than they are to detect in words from a person. An informed public should question and evaluate the veracity of the output of AI just as it should question the veracity of statements made by any person. Only if we are lazy and naïve and accept the output of AI as an absolute truth will we get into trouble. Perhaps we would all do well

to heed the words of Ronald Regan, who paraphrasing a Russian proverb, told us to "Trust but verify."

VI. **Will AI Turn Our Brains into Mashed Potatoes?**

Some predict that the better AI gets, the stronger NS will grow. That AI will displace thinking in human beings. That our reliance on the output of AI will cause us to engage in problem solving less and less and we will get dumber and dumber. They view a world in which our brains atrophy while the neural connections between mind, eye, and mouse click grow ever-stronger. I think that is a pessimistic view of the impact of new technology on human skill sets and behavior. It is a view that is recycled through history and continuously disproven. Slide rules were going to destroy a person's ability to do arithmetic. Ditto adding machines and calculators. Computers were going to displace the jobs of millions of workers and hasten our intellectual decline. None of which prophecies became true. Instead they were the predictions of persons, typically old persons, who were trying to graft new technology onto pre-existing activities. What these prognosticators failed to predict were the new activities brought into the world by the emerging technologies. New technology does not replace existing behavior; rather it creates new possibilities not foreseeable prior to the advent of new technology. It is the new possibilities that naysayers fail to consider.

Consider the impact of mapping technology. For centuries, people plotted the routes of their journeys using paper maps. Then came MapQuest which pre-printed guided routes for travelers to follow on their journeys; no longer did a person have to buy a map or plot their journey.. Then came the real-time, interactive, graphic technology of Google Maps and Waze that eliminated paper all together. In fact, they eliminated the necessity of keeping a draw stuffed with paper maps. Good-bye, or maybe hello to downsize, Rand-McNally. What was the impact of this technology? At first many felt that it would cause the map-reading neuronal cluster in our brain to atrophy which would then domino to overall stupidity and an inability to read anything, be it map or non-map. Embedded in this view was the belief, never fully articulated, that somehow a person was better off as map reader than as map non-reader: that map reading was a valuable and essential skill. Which may have been true when maps were needed. But they were no longer needed with the new technology. Perhaps those map reading skills that earned merit badges with the binary/boy/girl scouts were no longer essential. But, by ditching that rigorous mental exercise in lieu of mouse-clicks on a graphical map, did we become dumber? I don't think so. Instead, I think we became more adventurous and traveled to places we would not ever have travelled to before, because before it was too much of a hassle to read a map(s) to get there. So technology did not dumb us down, instead it educated us by enabling us to travel to new places and experience new things. Dare I say, it made the human experience more enjoyable?

VII. **Conclusion – We Can all Benefit from a dose of NSAIDs.**

Clearly the sentiments expressed in the above paragraphs are not without debate. Every sentence could be debated by advocates on both sides (assuming just two sides) of the views expressed. I believe a public dialog, a debate, about the benefits and drawbacks of AI should take place to create savvy, informed users. There should be a series of debates between those who believe in benefits of Natural Stupidity and those who believe in the benefits of Artificial Intelligence. The debates should be called the Natural Stupidity – Artificial Intelligence Debates or "NSAIDs". It is my hope that regular doses of NSAIDs, prescribed by industry authorities and consumed by an informed public, would cure the public of its irrational fears of AI, and reduce the high-temperature flare-ups between warring factions.

Federal Register
Vol. 90, No. 20
Friday, January 31, 2025

Presidential Documents

Title 3—

The President

Executive Order 14179 of January 23, 2025

Removing Barriers to American Leadership in Artificial Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. *Purpose.* The United States has long been at the forefront of artificial intelligence (AI) innovation, driven by the strength of our free markets, world-class research institutions, and entrepreneurial spirit. To maintain this leadership, we must develop AI systems that are free from ideological bias or engineered social agendas. 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, clearing a path for the United States to act decisively to retain global leadership in artificial intelligence.

Sec. 2. *Policy.* It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security.

Sec. 3. *Definition.* For the purposes of this order, ''artificial intelligence'' or ''AI'' has the meaning set forth in 15 U.S.C. 9401(3).

Sec. 4. *Developing an Artificial Intelligence Action Plan.* (a) Within 180 days of this order, the Assistant to the President for Science and Technology (APST), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (APNSA), in coordination with the Assistant to the President for Economic Policy, the Assistant to the President for Domestic Policy, the Director of the Office of Management and Budget (OMB Director), and the heads of such executive departments and agencies (agencies) as the APST and APNSA deem relevant, shall develop and submit to the President an action plan to achieve the policy set forth in section 2 of this order.

Sec. 5. *Implementation of Order Revocation.* (a) The APST, the Special Advisor for AI and Crypto, and the APNSA shall immediately review, in coordination with the heads of all agencies as they deem relevant, all policies, directives, regulations, orders, and other actions taken pursuant to the revoked Executive Order 14110 of October 30, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). The APST, the Special Advisor for AI and Crypto, and the APNSA shall, in coordination with the heads of relevant agencies, identify any actions taken pursuant to Executive Order 14110 that are or may be inconsistent with, or present obstacles to, the policy set forth in section 2 of this order. For any such agency actions identified, the heads of agencies shall, as appropriate and consistent with applicable law, suspend, revise, or rescind such actions, or propose suspending, revising, or rescinding such actions. If in any case such suspension, revision, or rescission cannot be finalized immediately, the APST and the heads of agencies shall promptly take steps to provide all available exemptions authorized by any such orders, rules, regulations, guidelines, or policies, as appropriate and consistent with applicable law, until such action can be finalized.

(b) Within 60 days of this order, the OMB Director, in coordination with the APST, shall revise OMB Memoranda M–24–10 and M–24–18 as necessary

to make them consistent with the policy set forth in section 2 of this order.

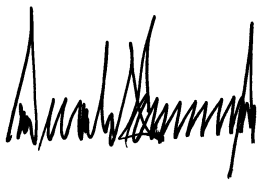
Sec. 6. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
January 23, 2025.

[FR Doc. 2025–02172
Filed 1–30–25; 11:15 am]
Billing code 3395–F4–P

Appendix C

December 11, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. United States leadership in Artificial Intelligence (AI) will promote United States national and economic security and dominance across many domains. Pursuant to Executive Order 14179 of January 23, 2025 (Removing Barriers to American Leadership in Artificial Intelligence), I revoked my predecessor's attempt to paralyze this industry and directed my Administration to remove barriers to United States AI leadership. My Administration has already done tremendous work to advance that objective, including by updating existing Federal regulatory frameworks to remove barriers to and encourage adoption of AI applications across sectors. These efforts have already delivered tremendous benefits to the American people and led to trillions of dollars of investments across the country. But we remain in the earliest days of this technological revolution and are in a race with adversaries for supremacy within it.

To win, United States AI companies must be free to innovate without cumbersome regulation. But excessive State regulation thwarts this imperative. First, State-by-State regulation by definition creates a patchwork of 50 different regulatory regimes that makes compliance more challenging, particularly for start-ups. Second, State laws are increasingly responsible for requiring entities to embed ideological bias within models. For example, a new Colorado law banning "algorithmic discrimination" may even force AI models to produce false results in order to avoid a "differential treatment or impact" on protected groups. Third, State laws sometimes impermissibly regulate beyond State borders, impinging on interstate commerce.

My Administration must act with the Congress to ensure that there is a minimally burdensome national standard — not 50 discordant State ones. The resulting framework must forbid State laws that conflict with the policy set forth in this order. That framework should also ensure that children are protected, censorship is prevented, copyrights are respected, and communities are safeguarded. A carefully crafted national framework can ensure that the United States wins the AI race, as we must.

Until such a national standard exists, however, it is imperative that my Administration takes action to check the most onerous and excessive laws emerging from the States that threaten to stymie innovation.

Sec. 2. Policy. It is the policy of the United States to sustain and enhance the United States' global AI dominance through a minimally burdensome national policy framework for AI.

Sec. 3. AI Litigation Task Force. Within 30 days of the date of this order, the Attorney General shall establish an AI Litigation Task Force (Task Force) whose sole responsibility shall be to challenge State AI laws inconsistent with the policy set forth in section 2 of this order, including on grounds that such laws unconstitutionally regulate interstate commerce, are preempted by existing Federal regulations, or are otherwise unlawful in the Attorney General's judgment, including, if appropriate, those laws identified pursuant to section 4 of this order. The Task Force shall consult from time to time with the Special Advisor for AI and Crypto, the Assistant to the President for Science and Technology, the Assistant to the President for Economic Policy, and the Assistant to the President and Counsel to the President regarding the emergence of specific State AI laws that warrant challenge.

Sec. 4. Evaluation of State AI Laws. Within 90 days of the date of this order, the Secretary of Commerce, consistent with the Secretary's authorities under 47 U.S.C. 902(b), shall, in consultation with the Special Advisor for AI and Crypto, the Assistant to the President for Economic Policy, the Assistant to the President for Science and Technology, and the Assistant to the President and Counsel to the President, publish an evaluation of existing State AI laws that identifies onerous laws that conflict with the policy set forth in section 2 of this order, as well as laws that should be referred to the Task Force established pursuant to section 3 of this order. That evaluation of State AI laws shall, at a minimum, identify laws that require AI models to alter their truthful outputs, or that may compel AI developers or deployers to disclose or report information in a manner that would violate the First Amendment or any other provision of the Constitution. The evaluation may additionally identify State laws that promote AI innovation consistent with the policy set forth in section 2 of this order.

Sec. 5. Restrictions on State Funding. (a) Within 90 days of the date of this order, the Secretary of Commerce, through the Assistant Secretary of Commerce for Communications and Information, shall issue a Policy Notice specifying the conditions under which States may be eligible for remaining funding under the Broadband Equity Access and Deployment (BEAD) Program that was saved through my Administration's "Benefit of the Bargain" reforms, consistent with 47 U.S.C.

1702(e)-(f). That Policy Notice must provide that States with onerous AI laws identified pursuant to section 4 of this order are ineligible for non-deployment funds, to the maximum extent allowed by Federal law. The Policy Notice must also describe how a fragmented State regulatory landscape for AI threatens to undermine BEAD-funded deployments, the growth of AI applications reliant on high-speed networks, and BEAD's mission of delivering universal, high-speed connectivity.

(b) Executive departments and agencies (agencies) shall assess their discretionary grant programs in consultation with the Special Advisor for AI and Crypto and determine whether agencies may condition such grants on States either not enacting an AI law that conflicts with the policy of this order, including any AI law identified pursuant to section 4 or challenged pursuant to section 3 of this order, or, for those States that have enacted such laws, on those States entering into a binding agreement with the relevant agency not to enforce any such laws during the performance period in which it receives the discretionary funding.

Sec. 6. Federal Reporting and Disclosure Standard. Within 90 days of the publication of the identification specified in section 4 of this order, the Chairman of the Federal Communications Commission shall, in consultation with the Special Advisor for AI and Crypto, initiate a proceeding to determine whether to adopt a Federal reporting and disclosure standard for AI models that preempts conflicting State laws.

Sec. 7. Preemption of State Laws Mandating Deceptive Conduct in AI Models. Within 90 days of the date of this order, the Chairman of the Federal Trade Commission shall, in consultation with the Special Advisor for AI and Crypto, issue a policy statement on the application of the Federal Trade Commission Act's prohibition on unfair and deceptive acts or practices under 15 U.S.C. 45 to AI models. That policy statement must explain the circumstances under which State laws that require alterations to the truthful outputs of AI models are preempted by the Federal Trade Commission Act's prohibition on engaging in deceptive acts or practices affecting commerce.

Sec. 8. Legislation. (a) The Special Advisor for AI and Crypto and the Assistant to the President for Science and Technology shall jointly prepare a legislative recommendation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order.

(b) The legislative recommendation called for in subsection (a) of this section shall not propose preempting otherwise lawful State AI laws relating to:

(i) child safety protections;

(ii) AI compute and data center infrastructure, other than generally applicable permitting reforms;

(iii) State government procurement and use of AI; and

(iv) other topics as shall be determined.

Sec. 9. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The costs for publication of this order shall be borne by the Department of Commerce.

DONALD J. TRUMP

THE WHITE HOUSE,

December 11, 2025.

Related

Removing Barriers to American Leadership in Artificial Intelligence

Presidential Actions | January 23, 2025

Fact Sheet: President Donald J. Trump Ensures a National Policy Framework for Artificial Intelligence

Fact Sheets | December 11, 2025

Advancing Artificial Intelligence Education for American Youth

Presidential Actions, Executive Orders | April 23, 2025

Unlocking Cures for Pediatric Cancer with Artificial Intelligence

Presidential Actions, Executive Orders | September 30, 2025

Reinvigorating America's Beautiful Clean Coal Industry and Amending Executive Order 14241

Presidential Actions, Executive Orders | April 8, 2025

1 2 3 ... 68 NEXT PAGE

U.S. AI Law Tracker

orrick

Which states have AI laws in effect today?

This tracker summarizes key AI laws that may impact your business. Information is only shown for states with defined laws. Please visit our AI Law Center for the latest information: orrick.com/ai

State/Terr	AI Scope	Relevant Law	Law Link	Effective Date	Key Requirements	Enforcements & Penalties
Alabama	AI CSAM	Alabama Child Protection Act of 2024	HB 168	October 1, 2024	• Expands the scope the definition of child sexual abuse material to include "virtually indistinguishable depictions" created, altered, or produced by digital, computer generated, or other means.	Existing criminal penalties apply.
Alabama	AI in Political Advertising	Alabama Materially Deceptive Election Media Law	AL HB172	October 1, 2024	• Prohibits the distribution of materially deceptive AI-generated media falsely depicting an individual that is intended to influence an election. • Provides a safe harbor from liability where the person provides a disclaimer that the media has been manipulated by technical means and depicts speech or conduct that did not occur.	• Class A Misdemeanor for first offense. • Class D Felony for subsequent offense.
Arizona	AI Intimate Images	Amendment of Arizona Intimate Images Law	Arizona Revised Statutes Section 13-1425	September 25, 2025	• Extends prohibitions on unlawful disclosure of intimate images to include realistic pictorial representations.	Class 1 Misdemeanor.
Arizona	AI Deepfakes	Arizona General Deepfake Law	HB 2394	June 4, 2024	Grants any Arizona citizen (or a candidate for public office or political party office who will appear on the ballot in Arizona) the right to bring an action for preliminary and permanent declaratory relief (and, in certain circumstances, injunctive relief or damages) where: • A digital impersonation (typically video, audio or still image generated by AI) of the person was published to one or more other persons without that person's consent; • At the time of publication it would not be obvious to a reasonable person that the content was a digital impersonation and the publisher did not reasonably convey to the recipients that the content was a digital impersonation or that its authenticity was disputed; and • The digital impersonation presents some risk of harm (e.g., depicting the person engaging in a criminal or sexual act, resulting in personal hardship or the loss of employment, presenting a risk to an upcoming election).	Permanent declaratory relief, permanent injunctive relief, and in certain circumstances, damages.
Arizona	AI in Political Advertising	Arizona Political Deepfake Law	SB 1359	June 4, 2024	• Prohibits any person from creating and distributing a synthetic media message that the person knows is a deceptive and fraudulent deepfake of a candidate for elected office within 90 days of an election unless the synthetic media message includes a clear and conspicuous disclosure that conveys to a reasonable person that the media includes content generated by artificial intelligence.	Permanent declaratory relief, permanent injunctive relief and, in certain circumstances, damages.

Arkansas	AI CSAM	Amendment of Arkansas CSAM Laws	HB1877	July 21, 2025	• Expands the scope of existing child pornography statutes to include AI generated images that are indistinguishable from the image of a child participating or engaging in sexually explicit conduct.	Existing criminal penalties apply.
Arkansas	AI Ownership	Ownership of Model Training and Generated Content	Arkansas Code Title 18-4-101	April 21, 2025	Sets the following default rules for AI ownership: • The person who provides input or directive to a generative AI tool is the owner of the generated content, provided the content does not infringe on existing copyrights or IP rights. • The person who provides data or input to train a generative AI tool is the owner of the resulting trained model, provided the training data was lawfully acquired and the person has not transferred ownership rights through a contract or agreement. • A person's employer will be deemed the owner of such generated content or resulting trained model where the person is employed and is directed to use a generative AI tool to conduct model training or generate content as part of their employment duties.	N/A
California	AI Calling	AI Call Disclosures Law	AB 2905	January 1, 2025	• Requires callers using an automatic dialing-announcing device to inform the person called if the prerecorded message uses an artificial voice generated or significantly altered using artificial intelligence.	Up to $500 per violation.
California	AI Definition	AI Definition Bill	AB 2885	January 1, 2025	• Generally establishes a uniform definition for artificial intelligence (AI) in California Law: "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments."	N/A
California	AI Healthcare	AI Healthcare Utilization Law	SB 1120	January 1, 2025	• Requires health care service plans and disability insurers that use an artificial intelligence, algorithm, or other software tool for the purpose of utilization review or utilization management functions to ensure compliance with specified requirements, including that the tool bases its determination on specified information and is fairly and equitably applied.	Criminal penalties.
California	AI CSAM	Amendment of California CSAM Laws	Cal. Penal Code Part 1; Title 9; Chapter 7.5 (311-312.7)	January 1, 2025	• Expands the scope of existing child pornography statutes to include matter that is digitally altered or generated by the use of AI.	Existing criminal penalties apply.
California	AI Intimate Images	Amendment of California Law Governing Distribution of Intimate Images	SB 926	January 1, 2025	• Extends prohibitions on the distribution of intimate images to include the intentional creation and distribution of any sexually explicit image of another identifiable person that was created in a manner that would cause a reasonable person to believe the image is an authentic image of the person depicted, under circumstances in which the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress.	Existing criminal penalties apply.

California	AI Likeness	Amendment to Deceased Personality Protections	AB 1836	January 1, 2025	• Makes it unlawful for a person to produce, distribute, or make available the digital replica of a deceased personality's voice or likeness in an expressive audiovisual work or sound recording without appropriate consent.	Greater of $10,000 or the actual damages suffered by a person controlling the rights to the deceased personality's likeness.
California	AI in Political Advertising	Amendment to the Political Reform Act	AB 2355	January 1, 2025	• Requires any committee that creates, originally publishes, or originally distributes a qualified political advertisement to include in the advertisement a specified disclosure that the advertisement was generated or substantially altered using artificial intelligence.	Up to $5,000 per violation.
California	AI Healthcare	Artificial Intelligence in Health Care Services	Cal. Gov. Code § Section 1339.75 AB 3030	January 1, 2025	• Requires health facilities, clinics, physician's offices, and offices of a group practice that uses generative AI to generate written or verbal patient communications pertaining to patient clinical information to ensure those communications include both: - A disclaimer that indicates to the patient that a communication was generated by generative artificial intelligence; and - Clear instructions describing how a patient may contact a human healthcare provider, employee, or other appropriate person. • Exempts from disclosure written communications that are generated by AI that are reviewed by a licensed or certified healthcare provider.	Existing regulatory enforcement mechanisms.
California	AI Transparency	Artificial Intelligence Training Data Transparency Act	AB 2013	January 1, 2026	• Requires AI developers to post information on the data used to train their generative AI on their websites, including a high-level summary of the datasets used, the sources or owners of the datasets, a description of how the data is used, the number of data points in the set, whether copyrighted / IP protected or licensed data is included, and the time period the data was collected (among other information).	Not specified.

California	User-Facing AI	California Companion Chatbot	Cal. Bus. & Prof. Code § 22601 et. seq.	January 1, 2026	• Requires operators of a "companion chatbot platform" to: - Issue a clear and conspicuous notification indicating that the chatbot is artificially generated and not human where a reasonable person interacting with the bot would be misled to believe that the person is interacting with a human; - Maintain and publish online details about a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to the user (including automated notification to the user that refers them to crisis service providers if they express such ideas); - Implement measures where the operator knows a user is a minor (under 18) to disclose that the user is interacting with AI, provide a clear and conspicuous notification at least every 3 hours that reminds the user to take a break and that the bot is AI, and institute reasonable measures to prevent the bot from producing visual material of sexually explicit conduct or directly stating the minor should engage in sexually explicit conduct; - Disclose on its platform that companion chatbots may not be suitable for some minors; and - Report annually on its compliance.	Provides a private right of action for anyone injured by a violation to seek injunctive relief, reasonable attorneys fees and damages in an amount equal to the greater of actual damages or $1,000 per violation.
California	AI Privacy	California Consumer Privacy Act	AB 1008	January 1, 2025	• Amends the definition of “personal information” under the CCPA to clarify personal information can exist in various formats, including, but not limited to, “abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.”	N/A
California	Automated Decision-Making	California Consumer Privacy Act Regulations	11 CCR § 7001 et seq.	January 1, 2027	Addresses the use of automated decision-making technology ("ADMT") when used to make significant decisions regarding consumers (those relating to financial or lending services, housing, education, employment, and healthcare): • Businesses must conduct a risk assessment when using ADMT to make significant decisions, or when using personal information to train ADMT. • Businesses that make ADMT (trained on personal information) available to another business to make a significant decision must provide to the recipient-business all facts available to the business that are necessary for the recipient-business to conduct its own risk assessment. • Businesses must provide pre-use notices to inform consumers about the use of ADMT, details about the ADMT, and the right to opt-out and access further information. • Businesses must allow consumers to opt out and provide consumers with access to information about the ADMT's use and logic. *Other obligations and restrictions may apply depending on the type of data processed*.	Up to $7,500 per violation.

California	AI in Social Media & Online Platforms	Digital Identity Theft Act	SB 981	January 1, 2025	Requires a social media platform to: • Provide a reasonably accessible mechanism to California users to report to the social media platform any sexually explicit image or video of them posted on that platform that was created or altered through digitization without their consent (i.e., “sexually explicit digital identity theft”); • Temporarily block any covered material from being publicly viewable on the social media platform pending the social media platform’s determination on the report; and • Removing any covered material from being publicly viewable on the social media platform once the platform determines there is a reasonable basis to believe the reported material is sexually explicit digital identity theft.	Not specified.
California	AI in Employment	Employment Regulations Regarding Automated-Decision Systems, issued pursuant to the California Fair Employment and Housing Act, Cal. Gov. Code § § 12935(a), 12940, 12941	Civil Rights Council Employment Regulations Regarding Automated-Decision Systems	October 1, 2025	Regulations clarify the application of existing antidiscrimination laws in the workplace in the context of new and emerging technologies, including AI that makes a decision or facilitates human decision making regarding an employment benefit ("Automated-Decision System"): • Employers must not use automated-decision systems that discriminate against applicants or employees on the basis of protected characteristics. • Employers must maintain employment records, including automated-decision system data, for a minimum period of four years.	Existing enforcement mechanisms.
California	AI in Government	Generative Artificial Intelligence Accountability Act	SB 896	January 1, 2025	• Requires the Office of Emergency Services to perform a risk analysis of potential threats posed by the use of GenAI to California’s critical infrastructure, and certain other state agencies / actors to take AI into account in various government processes. • Requires a state agency or department that utilizes generative AI to directly communicate with a person regarding government services and benefits to ensure that those communications include both (i) a disclaimer that indicates to the person that the communication was generated by generative artificial intelligence and (ii) describing how the person may contact a human employee of the state agency or department.	N/A
California	AI Healthcare	Health Advice From Artificial Intelligence	Cal. Bus. & Prof. Code § 4999.9	January 1, 2026	• Extends to AI technology providers pre-existing prohibitions on the use of any terms, letters, or phrases to indicate or imply (i) possession of a license or certificate to practice a healthcare profession without one or (ii) that the services being offered are being provided by a licensed or certified health care professional (where such claim is not true).	Appropriate health care professional licensing boards and enforcement agencies can take whatever action they authorized by law to take in response to such a violation.

California	AI in Government	Law Enforcement Usage of Artificial Intelligence	Cal. Civ. Code § 13663	January 1, 2026	• Requires law enforcement agencies to maintain a policy to require an official report prepared by the law enforcement agency (or one of its members) that is generated using AI either fully or partially to contain: - A disclosure on each page of the report (or within the body of the text) that the report was written either fully or in part using AI and the identity of every specific AI program used; and - The signature of the law enforcement officer or member who prepared the official report verifying that they reviewed the contents of the report and that the facts contained in the report are true and correct. • Requires law enforcement agencies who use AI to create an official report, whether fully or partially, to retain the first draft created and to maintain an audit trail for as long as the official report is retained. • Requires contracted vendors to not share, sell, or otherwise use information provided by a law enforcement agency to be processed by AI except for the contracted law enforcement agency's purposes or pursuant to a court order (with certain exceptions for accessing such data for troubleshooting, bias mitigation, accuracy improvement, or system refinement).	N/A
California	AI in Real Estate	Real Estate Digitally Altered Images Disclosures	Cal. Bus. & Prof. Code § 10140.8	January 1, 2026	• Requires real estate brokers, salespersons and persons acting on their behalf who include a digitally altered image (including AI altered images) in an advertisement or other promotional material for the sale of real property to include a statement disclosing that the image has been altered and a link to a publicly accessible internet website, URL, or QR code that includes, and clearly identifies, the original, unaltered image.	Disciplinary action under the California Real Estate Regulations, including potential revocation or suspension of real estate licenses.
California	AI Likeness	Replica of Voice or Likeness Law	AB 2602	January 1, 2025	• Makes any provision in an agreement for the performance of personal or professional services unenforceable where: - The provision allows for the creation and use of a digital replica of the individual's voice or likeness in place of work the individual would otherwise have performed in person; - The provision does not include a reasonably specific description of the intended uses of the digital replica; and - The individual was not represented (i) by legal counsel or (ii) by a labor union.	Unenforceability of a violating contractual provision.

Colorado	Automated Decision-Making	Colorado Privacy Act	Col. Rev. Stat. § 6-1-1301 et seq. *Reprinted from Westlaw with the permission of Thomson Reuters.*	July 1, 2023	• Provides consumers the right to opt-out of any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of solely-automated decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to essential goods and services). • Requires a data protection assessment of each processing activity involving such automated processing of personal data in certain circumstances. *Other obligations and restrictions may apply depending on the type of data processed.*	Up to $20,000 per violation.
Colorado	AI in Insurance	Colorado Protecting Consumers from Unfair Discrimination in Insurance Practices	Co. Rev. Stat. 10-3-1104.9 *Reprinted from Westlaw with the permission of Thomson Reuters.*	July 6, 2021	• Prohibits insurance providers from using algorithms or predictive models that unfairly discriminate based on race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression. • Requires the Colorado Commissioner of Insurance to adopt rules requiring insurers to demonstrate that their use of algorithms and predictive models do not result in unfair discrimination.	Up to $3,000 per violation, or $30,000 per knowing violation.
Colorado	AI CSAM	Preventing Unauthorized Disclosure of Intimate Digital Depictions Act	SB 288	August 6, 2025	• Expands child sexually exploitative material to include a realistic visual depiction, which has been created, altered, or produced by digitization or computer-generated means, that depicts an identifiable child, in whole or in part, engaged in, participating in, observing, or being used for explicit sexual conduct.	Plaintiffs may bring civil actions to obtain relief, and a court may order a temporary restraining order, injunctive relief, and order the defendants to cease disclosure.
Colorado	AI Intimate Images	Preventing Unauthorized Disclosure of Intimate Digital Depictions Act	SB 288	August 6, 2025	• Allows an individual depicted in an intimate digital depiction to sue the individual who disclosed or threatened to disclose the picture if they acted with knowledge or disregard for whether the depicted individual: did not consent to the disclosure; would experience serve emotional distress; and was identifiable. • Expands the scope of Colorado's intimate image harassment statute to include intimate digital depictions.	• For intimate digital depictions - the greater of actual damages or liquidated damages of $150,000, plus an amount equal to the monetary gain, exemplary damages, and the cost of the action; as well as equitable relief. • For intimate image harassment - existing criminal penalties apply.

Illinois	AI in Employment	Artificial Intelligence Video Interview Act	820 ILCS 42	January 1, 2020	• Requires employers who use AI to analyze applicant video interviews to notify each applicant of the use of AI, explain how the AI works, and obtain the applicant's consent prior to using the AI. • Requires employers who rely solely on AI to analyze video interviews to determine whether an applicant will be selected for an in-person interview to collect and report to the Department of Commerce and Economic Opportunity annually on the demographic data of the applicants	N/A
Illinois	AI Likeness	Digital Voice and Likeness Protection Act	HB 4762	August 9, 2024	• Makes any provision in an agreement for the performance of personal or professional services unenforceable where: - The provision allows for the creation and use of a digital replica of the individual's voice or likeness in place of work the individual would otherwise have performed in person; - The provision does not include a reasonably specific description of the intended uses of the digital replica; and - The individual was not represented (i) by legal counsel or (ii) by a labor union.	Unenforceability of a violating contractual provision.
Illinois	AI Healthcare	The Wellness and Oversight for Psychological Resources Act	HB1806	August 1, 2025	• Solely permits the use of AI tools or systems by a licensed professional where they are used to assist in providing administrative support or supplementary support in therapy or psychotherapy services and the licensed professional maintains full responsibility for all interactions, outputs, and data use associated with the system and satisfies the other requirements of the Act. • Prohibits licensed professionals from using AI to assist in providing supplementary support in therapy or psychotherapy where the client's therapeutic session is recorded or transcribed unless the patient is informed in writing of it's use and purpose and provides consent. • Prohibits licensed professionals from allowing AI to make independent therapeutic decisions; directly interact with clients in any form of therapeutic communication; generate therapeutic recommendations or treatment plans without review and approval; or detect emotions or mental states.	Up to $10,000 per violation.
Illinois	User-Facing AI	The Wellness and Oversight for Psychological Resources Act	HB1806	August 1, 2025	• Prohibits any individual or entity from providing, advertising, or otherwise offering therapy or psychotherapy services, including through the use of Internet-based artificial intelligence, to the public unless the therapy or psychotherapy services are conducted by an individual who is a licensed professional. • Exceptions are provided for religious counseling, peer support, and self-help materials and educational resources that are available to the public and do not purport to offer therapy or psychotherapy services.	Up to $10,000 per violation.
Indiana	AI Intimate Images	Amendment of Indiana Law Governing Distribution of Intimate Images	HB 1047	March 12, 2024	• Extends prohibitions on the distribution of intimate images to include computer generated images, including images of an individual created or modified by means of a computer software program, artificial intelligence, application, or other design editing tools.	Existing criminal penalties apply.

Kentucky	AI CSAM	Amendment to CSAM Law	HB 207	March 28, 2024	• Expands covered images under the Kentucky CSAM statutes to include "any visual depiction" that "has been created, adapted, or modified by a computer to appear to be an identifiable person." • Creates an exception under CSAM prosecutions to the "identifiable person" standard under which the Commonwealth need not prove "the actual identity or age of the minor, or that the minor actually exists."	Existing criminal and civil penalties apply.
Kentucky	AI Intimate Images	Amendment to Intimate Images law	HB 207	March 28, 2024	• Expands covered images under the Kentucky AI intimate images statute to include "any visual depiction" that "has been created, adapted, or modified by a computer to appear to be an identifiable person."	Existing criminal and civil penalties apply.
Kentucky	AI in Government	Government Use of AI Law	KRS 42.720 - 42.742	December 1, 2025	• Requires the Commonwealth Office of Technology to create an Artificial Intelligence Governance Committee to govern the use of AI systems by government agencies. • Gives the Commonwealth Office of Technology the powers to establish, publish, maintain, and implement comprehensive policy standards and procedures for the responsible, ethical, and transparent use of generative artificial intelligence systems and high-risk artificial intelligence systems by departments, agencies, and administrative bodies. • Requires government agencies to disclose to the public, through clear and conspicuous disclaimer, when AI systems are used for certain purposes. • Requires government agencies to disclose certain information and make available options for individuals to appeal when an AI system is used to make external decisions about them.	N/A
Kentucky	Automated Decision-Making	Kentucky Consumer Data Protection Act	Ky. Rev. Stat. § 367.3611 et seq.	January 1, 2026	• Provides consumers the right to opt-out of any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial or lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, or access to basic necessities, like food and water). • Requires a data protection assessment of each processing activity involving such automated processing of personal data in certain circumstances. *Other obligations and restrictions may apply depending on the type of data processed*.	Up to $7,500 per violation.
Louisiana	AI Intimate Images	Louisiana AI Intimate Image Law	14 La. Rev. Stat. Ann. § 73.14	August 1, 2024	• Makes it unlawful for any person, with the intent to coerce, harass, intimidate, or otherwise act maliciously, to disseminate or sell any video or still image created by AI that depicts another person intimately when the person disseminating the video or still image knows or has reason to know that he is not licensed or authorized to do so.	Up to 6 months imprisonment and/or $750 fine.

Louisiana	AI Intimate Images	Louisiana Deepfake Law	14 La. Rev. Stat. Ann. § 73.13	August 1, 2023	• Makes it unlawful for any person who, with knowledge that the material is a deepfake that depicts another person, without consent of the person depicted, engaging in sexual conduct, knowingly advertises, distributes, exhibits, exchanges with, promotes, or sells any sexual material.	Imprisonment for 5 – 30 years and a fine of not more than $50,000.
Louisiana	AI CSAM	Louisiana Deepfake Law	14 La. Rev. Stat. Ann. § 73.13	August 1, 2023	• Makes it unlawful for any person who, with knowledge that the material is a deepfake depicting a minor, knowingly creates or possesses material that depicts a minor engaging in sexual conduct.	Imprisonment for 5 – 30 years and a fine of not more than $50,000.
Maine	User-Facing AI	Communications with Consumers via AI	10 MRSA c. 239	September 24, 2025	• Prohibits any person from using an AI chatbot or any other computer technology to engage in trade and commerce with a consumer in a manner that may mislead or deceive a reasonable consumer into believing that the consumer is engaging with a human unless the consumer is notified in a clear and conspicuous manner that the consumer is not engaging with a human being.	Constitutes a violation of the Maine Unfair Trade Practices Act.
Maryland	AI Healthcare	AI Utilization Review	Md. Code Ann., Ins. §§ 15-10A-06, 15-10B-05.1	October 1, 2025	• Requires insurers, nonprofit health service plans, health maintenance organizations, dental plan organizations, and any other persons that provide health benefit plans subject to regulation by MD to submit to the Commissioner on a quarterly basis certain information relating to claims, including the number of adverse decisions by the carrier and whether an artificial intelligence, algorithm, or other software tool was used in making the adverse decision. • Further requires such covered entities to ensure that: - AI systems base their determinations on relevant clinical information and not solely on a group dataset; - Any criteria or guidelines for using an AI system complies with these requirements; - An AI system does not replace the role of a health care provider in the determination process under § 15-10B-07 (setting forth adverse decision procedures); - Use of AI does not result in unfair discrimination, and is otherwise fairly and equitably applied; - AI systems are open to inspection for audit or compliance reviews by the Commissioner; - Written policies and procedures are included in the utilization plan, including how an AI system will be used and what oversight will be provided; - The performance, use and outcomes of AI are reviewed and revised, if necessary and at least on a quarterly basis, to maximize accuracy and reliability; - Patient data is not used beyond its intended and state purpose, consistent with HIPAA; and - An AI system does not directly or indirectly cause harm to an enrollee, nor deny, delay or modify health care services.	Existing enforcement mechanism by the Maryland Insurance Commissioner apply.
Maryland	AI CSAM	Amendment to the Maryland CSAM Statute	MD. Code., Crim. Law 11-208	October 1, 2023	• Expands the definition of CSAM to include a computer generated image that is indistinguishable from an actual and identifiable child under the age of 16.	Existing criminal penalties apply.

Montana	AI Intimate Images	Privacy in Communications Law	MCA Section 45-8-213	October 1, 2025	• Expands offenses of violating privacy in communications to include possessing and threatening to disclose real or digitally fabricated sexual deepfakes with the purpose of obtaining money or other valuables.	Existing criminal penalties apply.
Montana	AI Likeness	Property Right in Use of Names, Voices, and Visual Likenesses	MCA Title 30, Chapter 14, Section 1	January 1, 2026	• Makes it unlawful for a person to intentionally publish, perform, distribute, transmit, or make available to the public a digital voice depiction or digital visual depiction for commercial use with actual or specific knowledge that the depiction is a digital voice depiction or digital visual depiction of the individual that was not authorized by the individual or the holder of the individual's property right (as well as distribution of any algorithm, software, tool, or other technology, service, or device with the actual and specific knowledge it will be used for such purposes).	A person who violates is liable to the injured person for the actual damages suffered by the person plus any profits from the unauthorized use of the individual's name, voice, or visual likeness.
Montana	AI in Critical Infrastructure	Right to Compute Act	SB212	April 16, 2025	• When critical infrastructure facilities are controlled in whole or in part by a critical AI system, the deployer must develop a reasonable risk management policy that considers guidance and standards in the NIST AI Risk Management Framework, the ISO/IEC 4200 AI standard, or another nationally or internationally recognized risk management framework for AI systems.	N/A
Nebraska	AI CSAM	Amendment of Nebraska CSAM Laws	LB 383	July 1, 2026	• Expands the definition of CSAM to include a computer generated image that is obscene and depicts a child, a person that would appear to a reasonable person to be a child, or a person depicted with physical features of a child.	Existing criminal and civil penalties apply.
Nebraska	Automated Decision-Making	Nebraska Data Privacy Act	LB 1074	January 1, 2026	• Provides consumers the right to opt-out of any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial or lending services, housing, insurance, healthcare services, education enrollment, employment opportunities, criminal justice, or access to basic necessities, such as food and water). • Requires a data protection assessment of each processing activity involving such automated processing of personal data in certain circumstances. *Other obligations and restrictions may apply depending on the type of data processed.*	Up to $7,500 for each violation.
Nevada	AI Healthcare	AI for Mental and Behavioral Health Care	Nev. Rev. Stat. Chapter 629	July 1, 2025	• Prohibits a provider of mental and behavioral health care from using an AI system in connection with providing professional mental and behavioral health care directly to a patient. • Expressly permits such a provider to use an AI system to assist the provider with performing tasks for administrative support.	A violation makes such a provider guilty of unprofessional conduct and subject to disciplinary action by the proper authorities.

Rhode Island	AI in Political Advertising	Deceptive and Fraudulent Synthetic Media in Election Communications	S.C. Code Ann. § 40-57-820	July 2, 2025	• Prohibits certain persons from distributing synthetic media that the person knows or should know is deceptive and fraudulent deepfake of a candidate for elected office within 90 days of an election unless the synthetic media message includes a clear and conspicuous disclosure stating that the media has been manipulated or generated by AI.	Provides possible injunctive or other equitable relief from injuries.
Rhode Island	Automated Decision-Making	Rhode Island Data Transparency and Privacy Protection Act	Tenn. Code. Ann. § 47-18-3301	January 1, 2026	• Provides consumers the right to opt-out of any form of solely automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to essential goods or services). • Requires a data protection assessment of each processing activity involving such automated processing of personal data in certain circumstances. *Other obligations and restrictions may apply depending on the type of data processed.*	Up to $10,000 per violation.
South Carolina	AI in Real Estate	Real Estate AI Responsibility Law	Chapter 2054, Government Code, Subchapter S	May 21, 2024	• Makes licensed real estate professionals responsible for any and all work product produced with the assistance of artificial intelligence, machine learning, or similar programs.	Various disciplinary actions and penalties.
South Dakota	AI CSAM	Amendment of South Dakota CSAM Laws	SB 20	February 12, 2024	• Expands the scope of existing child pornography statutes to include matter that is digitally altered or generated by the use of AI.	Existing criminal penalties apply.
South Dakota	AI in Political Advertising	An Act to Prohibit the Use of a Deepfake to Influence an Election	SB 1621	July 1, 2025	• Prohibits the distribution of AI-generated deepfakes with the intent to injure a candidate within 90 days of an election. • Provides a safe harbor from liability where the deepfake includes a disclosure stating "This (image/video/audio) has been manipulated or generated by artificial intelligence." The disclosure must also meet certain formatting / delivery requirements.	• Class 1 Misdemeanor. • Injunctive or other equitable relief. • Damages, reasonable costs and attorney fees, and any other relief the court deems proper in a suit by the candidate or other individual depicted.
Tennessee	AI CSAM	Amendment of Tennessee CSAM Laws	SB 815	July 1, 2024	• Expands the scope of existing child pornography statutes to include matter that is digitally altered or generated by the use of AI.	Existing criminal penalties apply.

Tennessee	AI Likeness	Ensuring Likeness, Voice, and Image Security (ELVIS) Act of 2024	SB 1188	July 1, 2024	• Provides that every individual has a property right in the use of their name, photograph, voice, or likeness in any medium and in any manner. • Establishes a civil cause of action if a person knowingly uses or infringes upon the use of an individual's name, photograph, voice, or likeness in any medium, in any manner, for purposes of advertising, fundraising, or merchandising without consent. • Establishes a civil cause of action if a person publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's voice or likeness with knowledge that the individual has not provided authorization for such use. • Establishes a civil cause of action if a person distributes, transmits, or otherwise makes available an algorithm, software, tool, or other technology, service, or device, the primary purpose or function of which is the production of an individual's photograph, voice, or likeness without authorization.	Private right of action.
Tennessee	Automated Decision-Making	Tennessee Information Protection Act	SB 2373	July 1, 2025	• Provides consumers the right to opt-out of any form of solely automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to basic necessities, like food and water). • Requires a data protection assessment of each processing activity involving such automated processing of personal data. *Other obligations and restrictions may apply depending on the type of data processed.*	Up to $7,500 per violation.
Texas	AI in Government	Act Relating to the Regulation and Use of AI by Governmental Entities	HB 441	September 1, 2025	• Requires Texas state agencies to inventory their AI systems and conduct a review of the deployment and use of heightened scrutiny AI systems. • Requires the creation for the state-wide establishment of an AI system code of ethics for use by state agencies and local governments that procure, develop, deploy, or use AI systems, which shall be adopted by the state agencies and local governments. • Requires the development of minimum risk management and governance standards for the development, procurement, deployment, and use of heightened scrutiny AI systems by a state agency or local government. • Requires state agencies to conduct assessments when deploying or using a heightened scrutiny AI system. • Requires state agencies to clearly disclose to an individual interacting with a public-facing AI system that they are interacting with an AI system, unless a reasonable person would know they are interacting with an AI system. • Requires state agencies to provide certain standardized notices of AI systems use that is public-facing or that is a controlling factor in a consequential decision.	The attorney general can enjoin a violation of the law and/or void a contract with a vendor causing such a violation.

Texas	AI Intimate Images	AI Sexual Material Harmful to Minors	HB 1999	September 1, 2025	• Commercial entities that operate a website with a publicly accessible tool for creating artificial sexual material harmful to minors, or otherwise makes publicly available an application for creating such material, must use reasonable age verification methods to verify an individual is 18 years of age or older. • Commercial entities providing such a tool or application must also ensure that an individual used as a source for the material is 18 years of age or older and has consented to the use of the individual's face and body as a source for the material.	Civil penalty of up to $10,000 per day it operates in violation of the age verification requirements or per instance of certain other violations, and up to $250,000 if a minor accesses sexual material because of a violation.
Texas	AI CSAM	Amendment of Texas CSAM Laws	SB 198	September 1, 2023	• Expands the scope of existing child pornography statutes to include matter that is digitally altered or generated by the use of AI.	Existing criminal penalties apply.
Texas	AI CSAM	Amendment to the CSAM Statutes	HB 441	September 1, 2025	• Expands the offenses of possession of child pornography, electronic transmission of certain visual material depicting a minor, and possession or promotion of lewd visual material depicting a child to include AI-generated images.	Felony offense.
Texas	AI Healthcare	Artificial Intelligence in Electronic Health Record	HB 2700	September 1, 2025	• Grants health care practitioners the ability to use artificial intelligence for diagnostic purposes, including using artificial intelligence for recommendations on a diagnosis or course of treatment based on a patient's medical record, if given conditions are met. • Provides a health care practitioner using artificial intelligence for diagnostic purposes must disclose the practitioner 's use of that technology to the practitioner's patients.	Injunctive relief and civil penalties of up to $5,000 for each violation that is committed negligently in a single year, $25,000 for each violation that is committed knowingly or intentionally in a single year, and $250,000 for each violation in which the covered entity knowingly or intentionally used protected health information for financial gain.
Texas	AI Deepfakes	Financial Abuse Using Artificially Generated Media or Phishing	HB 149	September 1, 2025	• Prohibits any person from intentionally or knowingly disseminating artificially generated media or a phishing communication for the purpose of financial exploitation. • Provides that a person commits an offense if the person knowingly engages in financial abuse through the use of artificially generated media disseminated to another person or by deceiving or manipulating another person into providing personal, financial, or identifying information through e-mail, electronic communication, or other digital means.	• Actual damages, damages for mental anguish, and the defendant's profits, as well as court costs and reasonable attorney's fees. • Civil penalty not to exceed $1,000 per day the media or communication is disseminated. • Criminal penalties and imprisonment can also apply.

Texas	AI Intimate Images	Unlawful Production or Distribution of Certain Sexually Explicit Material	HB 1999	September 1, 2025	• Expands what constitutes an unlawful production or distribution of certain sexually explicit visual material to include media that appears to depict a person with certain forms of intimate parts or performing certain actions without the person's consent. • Establishes liability for owners of internet websites, artificial intelligence applications, and payment processors involved in such artificial sexual material under certain conditions, and requires persons who own an Internet website or application to make available on the website or application an easily accessible system that allows a person to submit a request for the removal of such artificial material.	Establish the criminal penalties; Class B or Class A misdemeanor or a third degree felony.
Texas	AI Intimate Images	Unlawful Distribution of Sexually Explicit Videos	Wy. Code § 6-4-306	September 1, 2023	• Makes it a criminal offense to distribute deepfakes depicting a person with intimate parts exposed or engaged in sexual conduct without that person's consent.	Class A misdemeanor.
Texas	AI Healthcare	Use of Automated Decision System for Adverse Determinations	SB 1361	September 1, 2025	• Amends the Insurance Code to prohibit a utilization review agent from using an automated decision system, including certain AI systems, to make, wholly or partly, an adverse determination (i.e., a determination by a utilization review agent that health care services provided or proposed to be provided to a patient are not medically necessary or appropriate or are experimental or investigational).	Sanctions, cease and desist orders, and administrative penalties under the Insurance Code.
Texas	AI CSAM	Visual Material Appearing to Depict a Child	HB 581	September 1, 2025	• Creates a felony offense of possessing, accessing, or promoting obscene visual material of a child, regardless of whether the image is an actual child or created using artificial intelligence, or uses an image of a child with intent to train artificial intelligence to produce material constituting child pornography.	Felony offense.
Utah	AI Healthcare	AI Applications Related to Mental Health	Utah Code § 13-72a-101	May 7, 2025	• Prohibits the supplier of a mental health chatbot from: - Selling or sharing with any third party any individually identifiable health information of a Utah user or user input of a Utah user (with narrow exception). - Using a Utah user's input to facilitate targeted advertising. - Advertising a specific product or service to a Utah user in a conversation unless an appropriate disclaimer is provided identifying the relevant advertisement and any agreement / sponsorship to promote it. • Requires a mental health chatbot to clearly and conspicuously disclose that it is an AI technology (and not a human) to users before they begin to use the chatbot, upon commencement of any chatbot session (if the user has not accessed the chatbot within the previous 7 days), and whenever a user asks whether they are interacting with AI.	Fines of up to $2,500 per violation of the law, or $5,000 per violation of an order issued for a violation of the law.
Utah	AI Liability	Artificial Intelligence Consumer Protection Amendments	Utah Code § 13-75-102	May 7, 2025	• Clarifies that it is not a defense to a violation of Utah's consumer protection law that generative AI made the violative statement, undertook the violative act, or was used in furtherance of the violation.	Existing penalties apply.

Utah	AI Privacy	Utah Artificial Intelligence Policy Act	SB 149	May 1, 2024	• Clarifies that data generated by computer algorithms or statistical models that do not contain personal data (i.e., synthetic data) is not "personal data" under the Utah Consumer Privacy Act.	N/A
Utah	AI in Political Advertising	Utah Information Technology Act	SB 131	May 1, 2024	• Requires any person who uses generative AI to create audio or visual content intended to influence an election or ballot proposition to make clear disclosures including a disclaimer indicating the content is generated by AI.	$1,000 per violation recoverable by any person bringing a claim against the relevant creator or sponsor of the political content.
Vermont	AI Intimate Images	Amendment of non-consensual sexual image dissemination statute	Wy. Code § 6-4-306	June 6, 2024	• Expands the scope of Vermont's dissemination of intimate images statute to include media that has been altered "utilizing an image or images of a person, including images other than the person depicted, or computer-generated images."	Existing penalties apply.
Vermont	AI in Government	An Act Relating to the Use and Oversight of AI in State Government	H 410	July 1, 2022	• Requires the Agency of Digital Services to conduct an inventory of all the automated decision systems developed, employed, or procured by the Vermont State government. • The act also creates various AI governance functions within the Vermont State government.	None specified.
Virginia	AI CSAM	Amendment to CSAM statute	SB 731	July 1, 2024	• Clarifies that the definition of CSAM includes computer generated images of minors that do not "actually exist."	None specified.
Virginia	AI Intimate Images	Amendment to the Unlawful Dissemination of Images of Another Statute	B 2678	July 1, 2019	• Expands the definition of unlawful dissemination of nude or sexually explicit images of another to include persons "whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic."	None specified.
Virginia	AI in Government	Artificial Intelligence-Based Tools	Code of Virginia, Section 19.2-11.14	June 6, 2025	• Requires that all decisions related to the pre-trial detention or release, prosecution, adjudication, sentencing, probation, parole, correctional supervision, or rehabilitation of criminal offenders in Virginia must be made by a human decision-maker, even if artificial intelligence-based tools are used to generate recommendations or predictions. • Permits the use of any recommendation or prediction from an AI-based tool to be subject to any challenge or objection permitted by law.	N/A
Virginia	AI Healthcare	Hospital / Nursing Home Virtual Assistant Law	Va. Code Ann. § 32.1-127	July 1, 2021	• Mandates regulations to be adopted that require each hospital, nursing home, and certified nursing facility to establish and implement policies to ensure the permissible access to and use of an intelligent personal assistant provided by a patient while receiving inpatient services.	None specified.

Virginia	Automated Decision-Making	Virginia Consumer Data Protection Act	Va. Code Ann. § 59.1-577A(A)(5)	January 1, 2023	• Provides consumers the right to opt-out of any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, or access to basic necessities like food and water). • Imposes additional consent requirements and processing restrictions for such automated processing of children's personal data (under the age of 13). • Requires a data protection assessment of each processing activity involving such automated processing of personal data. *Other obligations and restrictions may apply depending on the type of data processed.*	Up to $7,500 per violation.
Washington	AI Intimate Images	Amendment of Washington Intimate Image Laws	Wy. Code § 6-4-306	June 6, 2024	• Makes it a criminal offense to knowingly disclose a fabricated intimate image of another person where the person disclosing the image knows or should have known that the depicted person has not consented to the disclosure and knows or reasonably should know that disclosure would cause harm to the depicted person.	Criminal and civil penalties may apply.
Washington	AI CSAM	Amendment of Washington CSAM Laws	Wy. Code § 6-4-306	June 6, 2024	• Expands the scope of existing child pornography statutes to include circumstances involving fabricated depictions of an identifiable minor (including such depictions created using AI).	Criminal and civil penalties may apply.
West Virginia	AI CSAM	Crimes Against Chastity, Morality and Decency - CSAM	Wy. Code § 6-4-306	July 9, 2025	• Expands prohibition on child pornography to include computer-generated child pornography.	Criminal and civil penalties may apply.
West Virginia	AI Intimate Images	Crimes Against Chastity, Morality and Decency - Intimate Images	Wy. Code § 6-4-306	July 9, 2025	• Expands prohibition on the distribution of intimate images to include fabricated intimate images created using AI or other computer technology.	Criminal and civil penalties may apply.
Wisconsin	AI in Political Advertising	2023 Wisconsin Act 123	Wis. Stat. § 11.1303	March 23, 2024	• Requires any political advertisement that contains express advocacy or issue advocacy, or supports or opposes a referendum, and incorporates audio or video content that is substantially produced in whole or in part by means of generative artificial intelligence to include a disclaimer indicating the content was created in whole or in part with the use of generative AI.	$1,000 per violation.
Wisconsin	AI in Real Estate	Advertising Enhanced by Technology Law	Wis. Stat. § 452.136(1m)	January 1, 2027	• Requires a person licensed to do real estate under Wisconsin law to disclose if a real estate advertisement has been altered or modified using technology, including artificial intelligence, to add, remove, or change elements of the property that creates a false or misleading impression of the property.	Suspension or revocation or real estate license and up to $5,000 per violation.

Appendix E

Art. 22 GDPR

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Suitable Recitals

(**71**) Profiling, (**72**) Guidance of the European Data Protection Board Regarding Profiling, (**91**) Necessity of a Data Protection Impact Assessment

GDPR Curbs Use of AI Via Article 22 Decision

Andrew Pery, **Michael Simon**

January 2024

Introduction

For years, **GDPR Article 22**, "Automated individual decision-making, including profiling," has been something of the forgotten Article. Even as AI has become a bigger and bigger issue – perhaps now the *only* issue – and despite the obvious direct connection between AI and Article 22, it has remained largely unused, until now. That's because on December 7, 2023, the Court of Justice of the EU (CJEU), in **Case C-634/21|SCHUFA Holding (Scoring)**, gave new life to Article 22 by holding that credit scoring is "profiling" and that the credit agency must obtain data subject consent by doing so. The CJEU thus ended years of controversy over whether Article 22 presents an inherent right for all EU citizens or an invocable right that becomes applicable on demand. By holding that Article 22 is an inherent right, the CJEU has brought Article 22 to the forefront at exactly the time that it is most needed, to provide a potential curb to abuses of AI and algorithmic decision-making.

Article 22 Was the Forgotten Right in GDPR

Unlike many other articles in GDPR, Article 22 is sufficiently brief to copy and paste herein:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

   a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   b. is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   c. is based on the data subject's explicit consent.

> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
>
> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 22 sits at the penultimate end of one of the most important sections of the GDPR: Chapter 3, Data Subject Rights, which covers such well-known and often-used rights as the Right to Access in Article 15 and the Right to Data Erasure (Right to Be Forgotten), in Article 17. Yet those other, far-more-famous rights in Chapter 3 are clearly invocable rights; an organization must only provide access to your personal data or delete it after making a data subject access request (DSAR) for them to do so. Thus, it was easy for everyone to view Article 22 as a continuation of that trend in Chapter 3, that it is an invocable right that lies dormant until a data subject makes a DSAR specifically on that subject. But because it would be nearly impossible to actually invoke such a right, it was also easy for everyone to believe that Article 22 was dead.

Indeed, a May 2022 **report** from the Future of Privacy Forum ("FPF"), "Automated Decision-Making Under the GDPR: Practical Cases from Courts," showed just how little Article 22 was actually used by claimants and the courts. Going back to pre-GDPR principles, such as Article 15 of the EU Data Protection Directive, EU 95/46 (which the GDPR superseded in 2018) and even before then back to the 1970s, the FPF report found only 19 cases and 50 enforcement actions premised upon Article 22.

The FPF report tries to put a good spin on this highly limited use of Article 22, stating in the introduction that "it now looks like individuals are increasingly interested in having their right under Article 22 applied." However, more than a few of the cases that the FPF reports upon have little or even nothing to do with determinations on Article 22. In fact, the FPF report contains an entire sub-section of cases that apply *other* rights within the GDPR to automated decision-making or profiling and wholly ignore Article 22.

And yet, the FPF report also contained a premonition of the recent developments that have now, almost undisputedly, bought Article 22 back into focus:

> Like for other provisions of EU law, the CJEU has ultimate authority to interpret Article 22 GDPR, but it has not yet adjudicated on its content. Questions for a preliminary ruling to clarify the content and scope of Article 22 GDPR have been sent to the CJEU in 2021 by the Administrative Court of Wiesbaden (Germany) in the SCHUFA case (C-634/21), and by the Vienna Regional Administrative Court (Austria) in February 2022.

The FPF report even covered the SCHUFA case as Case Number 39:

> Case 39: Request for a CJEU preliminary ruling — Can an automated credit score created by a credit reference agency which is later shared with third parties be qualifying ADM? In this case, the Wiesbaden Court is called upon to assess the business model of German credit reference agency SCHUFA — which is providing its clients (e.g. banks) with information on the creditworthiness of consumers through so-called score values— against GDPR provisions. The Court seems to take the preliminary view that the upstream credit scoring automated process itself — and not merely the downstream decisions taken on basis of such score (e.g., to automatically reject a loan application)— goes beyond mere profiling, as it decisively influences subsequent decisions that significantly affect data subjects. Through the way it drafted the questions, it seemed that the referring Court intended to obtain confirmation from the CJEU on whether credit scoring can amount to an automated decision which is prohibited under Article 22 GDPR.

The EDPB May Have Thought That It Had The Final Word, Except That Pretty Much Everyone Ignored It

From the very beginning of the issuance of the final GDPR text, even before it became effective, there has been debate over whether Article 22 contains an invocable or an inherent right. For example, a group of Oxford researchers argued that Article 22 needed to be an inherent right to be in any way effective. Yet this research was quickly countered by yet another group of Oxford researchers who argued just as persuasively that Article 22 contained an invocable right.

The text of Article 22(1) appears to support the view that it contains an inherent right; "The data subject shall have the right not to be subject to a decision . . ." does not contain any mention of a requirement for action on the part of the data subject. Compare this to the actionable statements in, for example, Article 15, the Right to Access, "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, . . ." and Article 17, the Right to Erasure, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her" (emphasis added for both) – which both contain the verb "to obtain." The passively-stated language in the first part of GDPR Recital 71 appears to further support the view that Article 22 contains an inherent right:

> The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Turning to the interpretation of the language of Article 22, GDPR Recital 72 states, in its second part, that "The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context," and indeed it has done so, at least in its pre-GDPR incarnation as the Article 29 Data Protection Working Party ("Working Party"). On October 3, 2017, the Working Party gave its interpretation of Article 22, in its "**Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**" (revised and updated on February 3, 2018, but not substantively changed):

> The term right in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data.

Just in case that was not sufficiently clear the first time, the Working Party Guidelines repeat:

> As explained earlier in this chapter, Article 22(1) acts as a prohibition on solely automated individual decision-making, including profiling with legal or similarly significant effects. Instead of the data subject having to actively object to the processing, the controller can only carry out the processing if one of the three exceptions covered in Article 22(2) applies.

Thus, with the stroke of a pen (at least metaphorically), the Working Party designated Article 22 as an inherent right. Or at least perhaps they thought that they did.

It is difficult to overstate the degree of surprise and push-back that met this pronouncement. We don't have the room in this article to cover all of these objections, so we will focus on those from the **International Association of Privacy Professionals** ("IAPP") and **Eduardo Ustaran,** the partner at Hogan Lovells who has been the lead author of the IAPP's testing materials and guidebook on the Certified Information Privacy Professional – EU for years. The IAPP quoted Ustaran as casting very strong doubt upon the Working Party's Guidelines:

> I think that regarding Article 22(1) as an outright prohibition is not entirely in line with the risk-based approach of the GDPR, said Ustaran, who warned of "considerable uncertainty" for industry in a recent article on the subject.

There's an old saying from the 1960's: "what if they gave a war and nobody came?" While, sadly enough, we still don't know the answer to that, we do know what the answer to the equivalent for "what if they

wrote a regulation and nobody followed it" is: eventually the courts will make everyone follow it. And the time for that for Article 22 may well be now.

The CJEU Has Now Removed All Doubt – And Any Room To Ignore The EDPB – By Holding That Article 22 Is An Inherent Right

Case history

Schufa Holding AG is the singular Germany credit rating agency that holds information on 68 million individuals and ranks them with a proprietary Schufa score. Think of Schufa as a combination of Equifax, Experian, and Transunion – with FICO added into the equation as well. A German resident who was turned down for a bank loan on the basis of a low Schufa score challenged the decision and the profiling behind that decision to the Hessian state data protection authority (DPA). The case was then referred by the Administrative Court of Wiesbaden to the CJEU for a ruling on the GDPR issues.

The CJEU opinion on this subject is short, just two pages long, and the portion dealing with Article 22 even shorter, just a single paragraph:

> As regards 'scoring', the Court holds that it must be regarded as an 'automated individual decision' prohibited in principle by the GDPR, in so far as Schufa's clients, such as banks, attribute to it a determining role in the granting of credit. According to the Administrative Court of Wiesbaden, this is the case. It is for that court to assess whether the German Federal Law on data protection contains a valid exception to that prohibition in accordance with the GDPR. If this is the case, it will still have to check whether the general conditions laid down by the GDPR for data processing have been met.

And so, with this single paragraph, the CJEU has revived Article 22 from a largely dead issue into a pivotal problem for any organization using automated decision-making systems. Since such systems are at the heart of so many AI use cases, especially the most profitable ones, the decision does not just resurrect Article 22, but transforms it into what is now potentially the main enforcement hook for regulators as to such AI systems.

NOYB - the EU public interest privacy organization founded by activist Max Schrems **quotes one of its member activists, Marco Blocher** for the potentially massive implications here: "Simply assigning citizens an incomprehensible credit score and then automatically refusing contracts is a thing of the past thanks to the CJEU judgment." But the impact of this decision does not stop there; as **one international law firm calls it a "watershed moment,**" for the delicate balance between AI innovation and privacy rights.

Where Do We Go From Here?

While the first part of Recital 72 specifically calls out "online credit applications" (such as Schufa) and "e-recruiting practices," as specifically subject to Article 22 the next section of the Recital greatly expands that list of applicable examples:

> Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

Thus, any industry that uses automated decision-making or profiling, including AI that accesses or even potentially has been trained upon personal data – which is, frankly, typically the most common and most valuable form of AI, must now quickly revamp any privacy program that previously ignored Article 22 to adapt to its requirements:

- If the organization wishes to exempt itself from the Article by using "human-in-the-loop" decision-making, so as not to be a "decision based solely on automated processing" under Part (1), it must be ready to demonstrate that the looped-in humans have the required training, experience and capabilities to truly review and where necessary override the AI system's decision-making. The FPF report makes clear that while there are few decisions concerning Article 22, those courts who have reviewed human-in-the-loop claims have been highly skeptical of "human-washing" AI determinations with systems that allow for little or no actual involvement, review or autonomy of those humans over the machine;

- If the organization wishes to use one of the exceptions in Part (2), it must tread carefully to avoid such common Article 6 lawful purposes that were explicitly left out of exceptions, particularly "legitimate interest." The only three possible exemptions come from:

  - "Necessary for entering into, or performance of, a contract between the data subject and a data controller." This is not nearly as large a loophole as it seems; while we do not have any specific decisions or guidance on this provision in Article 22, we do have such for the analogous provision in Article 6(1)(B), which sets out contractual necessity as a lawful basis for processing. **The EDPB Guidelines 2/2019 "on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**" make it clear that "necessary" is to be interpreted absolutely strictly and objectively: "The controller should be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur." Lack of that strict, objective necessity is what tripped up **Meta in December, 2022,** in its attempt to gain CJEU approval for contractual necessity for a lawful basis.

As well, credit scoring presents a further difficulty here, in that the controller doing the processing for the credit scoring is *not* the controller entering into the contract with the data subject. In fact, one has to wonder whether *any* data subject has ever actually specifically entered into a contract with a credit scoring agency or how one could actually do so.

○ Authorization by an EU Member State law to which the controller is subject, but which also contains "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;" or

○ "Explicit consent." It is important to note that, per the FPF report, that this is *not* the "usual" type of consent covered by Articles 4(11), 6(1)(a) and 7, but instead, per EDPB clarification, something that entails additional efforts from controllers to obtain. Further, some situations simply do not allow for the use of even non-explicit consent, including the general German ban on the use of consent in employment-related situations. Even if you can obtain consent here – which again seems doubtful in scenarios like credit scoring – Article 7(3) mandates that the data subject must be allowed to withdraw consent at any time.

• If the organization uses either contractual necessity or explicit consent as an exemption, it will also need, as per Part (3) to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." The Working Party Guidelines highlight that Recital 71 includes some short examples of safeguards that should apply "in any case": ".. specific information to the data subject ..... to obtain an explanation of the decision reached after such assessment and to challenge the decision." Moreover, in one of those rare EU decisions that cites to Article 22, the Garante (the Italian DPO), in its July 22, 2021, decision against Deliveroo has provided some additional thoughts on what could constitute such suitable measures:

. . . it does not appear that the company, in relation to the processing carried out as owner, has adopted technical and organizational measures to protect the interested parties aimed at periodically verifying the correctness and accuracy of the results of the algorithmic systems, the accuracy, relevance and adequacy of the data used by the system with respect to the purposes pursued, and to reduce as much as possible the risk of distorted or discriminatory effects, with reference to the functioning of the digital platform.

• Finally, per Part (4) if the organization processes any special categories of personal data referred to in Article 9(1)(i.e., "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation") it will need to either obtain "explicit consent" (again, not just regular consent) under Part (2)(a) or show that the processing is necessary for the public interest

under Part (2)(g) *and* also put into place "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."

Conclusion: Perhaps We Should Have Seen This Coming All Along?

Long before this CJEU ruling and just soon after GDPR became effective, **two leading Oxford Internet Institute researchers showed how GDPR would become a critical means to regulate not just privacy, but also AI**: "As applications of AI become more pervasive protected categories of personally identifiable information are expected to encompass inferences, predictions, and assumptions that refer to or impact an individual... under data protection law." The authors of the paper, who were solidly on the "Article 22 is an inherent right" side of inherent/invocable debate, argue the need for a new data protection right the "right to reasonable inferences...to help close the accountability gap currently posed by "high-risk inferences," meaning inferences drawn through Big Data analytics that are privacy-invasive or reputation-damaging."

The Schufa Holding AG case is an indication of the courts' willingness to expand the scope of protectable personal information to include inferred data that harms the economic and reputational rights of data subjects in exactly the way that was predicted all along.

Search for...

The EU AI Act: What Life Sciences and Digital Health Companies Should Know

4 minute read | September.13.2024

This update is part of our EU AI Act Series. Learn more about the EU AI Act here.

Life sciences and digital health companies face obligations under the AI Act that vary depending on how they use AI – and the level of risk involved.

The Act classifies some AI use cases in life sciences and digital health as high risk, such as when companies use AI in medical devices or in-vitro fertilization. Those uses subject companies to heightened regulation.

Companies that use AI in ways that carry lower risk face fewer obligations. Examples include using AI in drug discovery, non-clinical research and development and earlier stage clinical trials.

Higher Risk Uses Trigger Heightened Regulation

Medical devices incorporating AI systems may create risks not addressed by traditional regulatory requirements. The AI Act aims to fill some of those gaps, particularly in high-risk scenarios.

Whether AI systems are classified as high risk largely depends on the intent behind their use, considering whether they are used for clinical management of patients, such as diagnosing patients and informing therapeutic decisions, or in precision medicine.

These contexts typically fall under medical device regulation subject to third-party conformity assessment, giving rise to the high-risk use classification. Conformity testing requirements under device regulations may incorporate the requirements of the AI Act, but the Act will not itself impose additional requirements.

Lower Risk Classifications

Other AI or machine learning uses likely fall under lower risk classifications. Examples include companies that use AI in:

- Drug discovery applications, such as identifying potential targets and therapeutic pathways.
- Non-clinical research and development – using AI/ML modeling techniques to augment or replace animal studies, for example.
- Earlier stage clinical trials, where companies may use AI to analyze data and model future studies. (The European Medicines Agency takes a similar view in its draft guidance on using AI/ML in drug development.)

The Act's rules governing general purpose AI models (GPAIMs) and systems may affect other use cases. From a developer's perspective, these largely involve heightened transparency obligations, risk assessment and mitigation.

Governance Considerations

As AI/ML tools increasingly make their way into life sciences and digital health, deployers of these tools and companies using them must keep in mind the importance of responsible AI/ML practices. AI/ML users should adopt internal governance systems to ensure they:

- Obtain rights for data used to train models and adhere to any confidentiality obligations with respect to data sets used for training.
- Rely on diverse and reliable data sets to train models, particularly when there is higher potential for risk.
- Use AI/ML tools to augment and automate processes without minimizing the need for human oversight.

At a smaller scale, AI/ML tool deployers frequently must contend with pharma or biotech companies concerned about their data training models competitors may use.

How can AI/ML tool deployers continue providing services in life sciences and digital health despite these concerns?

They may consider sandboxing and firewalling data sets for engagements or running data sets through pre-trained models where the specific inputs are not used to train the overall model. The AI Act does not speak to these commercial or competitive considerations, adding another element for AI/ML deployers to navigate.

The Act does, however, provide for "regulatory sandboxes" where companies can test novel technologies under a regulator's supervision. The aim is to create controlled environments where companies can test and on-ramp technologies while regulators gain insight into how the technologies function prior to more widespread adoption by consumers.

What's Next?

The Act and input from the EMA helped clarify some high-risk, high-regulation scenarios and use cases involving AI/ML in life sciences and digital health. Yet many questions remain, from legal, regulatory and commercial perspectives.

Developers of AI/ML technologies should determine whether their technologies fall under the Act. They may also consider using regulatory sandboxes to ensure their product and service deployment aligns with regulators' evolving expectations.

Finally, given the increasing importance of AI, stakeholders should monitor legislative developments across jurisdictions as sector-specific laws begin to emerge.

Want to know more? Reach out to a member of our team.

Authors

Julia Apostle
Partner, Technology Transactions, Cyber, Privacy & Data Innovation

Paris

D +33153537500
E japostle@orrick.com

David Sharrow
Partner, Life Sciences & HealthTech, Technology Transactions

Boston

D +1 617 880 2053
E dsharrow@orrick.com

Related Areas

- **Artificial Intelligence (AI)**
- **Life Sciences & HealthTech**

Appendix H

European Commission

AI Act Service Desk

AI Act Explorer

CHAPTER III: HIGH-RISK AI SYSTEMS | Section 3: Obligations of Providers and Deployers of High-Risk AI Systems and Other Parties

Article 16: Obligations of providers of high-risk AI systems

Summary

Providers of high-risk AI systems must ensure their systems comply with the AI Act's requirements and have a quality management system in place. They must maintain documentation, keep logs, and undergo conformity assessments before market release. Providers must also issue an EU declaration of conformity, affix the CE marking, and comply with registration and accessibility requirements. They are responsible for taking corrective actions and demonstrating compliance to authorities upon request.

The summaries are meant to provide helpful explanation but are not legal binding.

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Section 2;

(b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted;

(c) have a quality management system in place which complies with Article 17 *(/en/ai-act/article-17)*;

(d) keep the documentation referred to in Article 18 *(/en/ai-act/article-18)*;

Page 66

(e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19 *(/en/ai-act/article-19)*;

(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43 *(/en/ai-act/article-43)*, prior to its being placed on the market or put into service;

(g) draw up an EU declaration of conformity in accordance with Article 47 *(/en/ai-act/article-47)*;

(h) affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with this Regulation, in accordance with Article 48 *(/en/ai-act/article-48)*;

(i) comply with the registration obligations referred to in Article 49(1) *(/en/ai-act/article-49)*;

(j) take the necessary corrective actions and provide information as required in Article 20 *(/en/ai-act/article-20)*;

(k) upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2;

(l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Relevant recitals

Recital 79 *(/en/ai-act/recital-79)* Recital 80 *(/en/ai-act/recital-80)* Recital 81 *(/en/ai-act/recital-81)* Recital 82 *(/en/ai-act/recital-82)* Recital 83 *(/en/ai-act/recital-83)* Recital 84 *(/en/ai-act/recital-84)* Recital 85 *(/en/ai-act/recital-85)* Recital 86 *(/en/ai-act/recital-86)* Recital 87 *(/en/ai-act/recital-87)* Recital 88 *(/en/ai-act/recital-88)* Recital 101 *(/en/ai-act/recital-101)* Recital 104 *(/en/ai-act/recital-104)* Recital 106 *(/en/ai-act/recital-106)* Recital 109 *(/en/ai-act/recital-109)* Recital 114 *(/en/ai-act/recital-114)* Recital 117 *(/en/ai-act/recital-117)* Recital 118 *(/en/ai-act/recital-118)* Recital 119 *(/en/ai-act/recital-119)* Recital 136 *(/en/ai-act/recital-136)* Recital 145 *(/en/ai-act/recital-145)*

View the official text. The text used in this tool is the 'Artificial Intelligence Act (Regulation (EU) 2024/1689), Official version of 13 June 2024'.

Appendix I

When AI Technology and HIPAA Collide

Posted By Todd Mayover on May 2, 2025

Minefields HIPAA Covered Entities and Business Associates Should Avoid

HIPAA Covered Entities beware! Your vendors are probably implementing artificial intelligence ("AI") technology within their service offerings.

Today, an all-too-common scenario involves an email message or telephone call from your trusted third-party vendor indicating that they are going to integrate AI technology into their service offerings that will involve the use of your patients' Protected Health Information (PHI). They claim that by using AI technology, they can provide their deliverables in less time, generate useful insights more rapidly, interpret medical imaging, improve the delivery of diagnosis and treatment, or perform accurate predictive analytics.

However, lurking surreptitiously behind the potential benefits of using PHI in AI technology lies a murky mix of risks that could negatively impact you, your vendors, and even your patients, especially when HIPAA compliance and patient PHI are involved. So how should a Covered Entity respond to its Business Associates' use of patient PHI in AI technology?

AI Technology

When assessing a Covered Entity's or Business Associate's use of PHI in AI technology, it is helpful to have a basic level of understanding of what is meant by AI technology. In layman's terms, AI is a machine's ability to undergo tasks that are typically performed by humans, or which require human intelligence.

One goal of AI is to create applications that are capable of being self-reliant and can think and act like humans. For example, an application that is able to perform tasks by learning and problem solving. AI technology involves the use of computer algorithms and analytics to build models that can solve problems. But in order for these models to be useful, the algorithms require enormous amounts of data to learn from.

Regulating Data When Using AI Technology

When AI technology uses large sets of data that are used to train the AI technology for their intended purposes, the data is likely going to include personal data, health data, or even PHI. Because the AI technology is using these types of data, data privacy laws and regulations will impact the AI technology's uses of that data. In other words, if the AI technology is using large amounts of PHI,

HIPAA will apply to the PHI, whether the AI technology is used by a Covered Entity or by a Covered Entity's Business Associates.

Consider the following scenario: a Covered Entity hires a data aggregator as its Business Associate to input large amounts of PHI from providers' electronic health records in order to train and use AI technology to identify diverse candidates for clinical trials. HIPAA will continue to apply to the PHI that is ingested by the AI technology because PHI is being collected from providers and is being used by the Business Associate's AI technology to provide services on behalf of the Covered Entity.

Issues When Using PHI with AI Technology

The most common issues to be aware of when using PHI in AI technology arise from the application of HIPAA's rules to the use of PHI with regard to the AI technology. Some of the issues may seem obvious – and that's partly the point. The application of HIPAA's rules will not vary, but there are many uses of PHI in AI technology, so the challenge is to understand how HIPAA's rules apply to the various uses of PHI by the AI technology. Here are a few examples of how HIPAA's rules can impact the uses of PHI in AI technology:

Authorization to Use PHI in AI Technology

The first issue to address is whether a Covered Entity or its Business Associates have the appropriate authority to use PHI in AI technology. Under the HIPAA Privacy Rule, there are explicit requirements regarding the access, collection, use, and disclosure of PHI.

Is the use for Treatment, Payment, or Healthcare Operations ("TPO")? Research? Marketing? Under the direction of a valid HIPAA authorization from the patients? Does it fall under any of the other approved uses under HIPAA that do not require an authorization (public interest, law enforcement, etc.)? These uses are all governed by the HIPAA Privacy Rule.

Where the use of PHI is not for TPO or another approved use without an authorization, the requirement to obtain a HIPAA authorization still applies for such uses as research, marketing, or any other use of the PHI pursuant to a valid HIPAA authorization.

Training AI technology may not be considered TPO, so if a Covered Entity or its Business Associates are interested in using large amounts of PHI for training purposes, they will first need to obtain an appropriate HIPAA authorization to do so from each patient. However, obtaining HIPAA authorizations from large numbers of individuals will be challenging, and this process could hinder the ability to input large amounts of PHI in AI technology.

Data Minimization and Purpose Limitation

An important limitation on the use of PHI under the HIPAA Privacy Rule is that a Covered Entity and its Business Associates must only use the minimum amount of PHI necessary for its intended purposes. There are a few exceptions to this rule, such as when one Covered Entity is sharing the PHI of a patient with another Covered Entity for treatment purposes, or when disclosing PHI directly to the patient. However, in most instances, when using PHI, only the minimum amount of PHI must be used for its intended purposes.

So how would a Covered Entity or its Business Associates address this requirement when using AI technology? If large amounts of PHI must be ingested by AI technology to train it, how much PHI is enough? Who would decide how much is enough? And is the PHI being used for its intended

purposes? Is someone going to oversee the use of PHI to ensure that the use does not violate the HIPAA Privacy Rule?

Another major concern about using PHI in AI technology is the ease with which the AI technology can access and use more data than is necessary for the intended purposes, e.g., data overreach. If a Covered Entity's Business Associates are going to use large amounts of PHI to train AI technology, it will be challenging to ensure that the Minimum Standard and Purpose Limitation are met while safeguarding against data overreach.

Role-Based Access to PHI When Using AI Technology

Under the HIPAA Security Rule, only those employees who have a need to access and use PHI as part of their roles should be given access to it. Thus, a Covered Entity and its Business Associates are required to have role-based access controls in place to ensure that only those employees who need to have access to PHI are able to do so.

This poses another challenge when working with AI technology as only the employees who have met the access control requirements should be working with PHI. Will this requirement change which roles are able to work with PHI and AI technology?

For smaller entities, it may be difficult to assign roles and rights to access and use PHI because employees may be required to perform several different functions within their job duties. For example, a start-up company that has lean engineering and data science teams may have employees that have multiple job functions that require access to various forms of data including both PHI and de-identified data.

Because of the smaller number of employees, it will be challenging to assign roles and responsibilities to employees who typically do not have access to PHI, but work with AI technology, to now do so while also maintaining independence from access to de-identified data. This is a problem because employees who work with de-identified data should not work with PHI and vice versa in order to avoid instances where de-identified data could be re-identified by an employee who also works with PHI.

Data Integrity and Confidentiality

Another HIPAA Security Rule requirement is that a Covered Entity and its Business Associates must ensure the integrity, confidentiality, and availability of PHI. Therefore, when using PHI in AI technology, strict security measures must be in place to adequately protect the integrity, confidentiality, and availability of the PHI. Such measures should include at a minimum: access controls, encryption, firewalls, and continuous monitoring and oversight of the use of PHI by the AI technology to prevent unauthorized access to or use of the PHI.

However, it will be more difficult to implement and ensure there are appropriate security controls in place in the AI technology, if the AI technology is pulling in and using data from multiple sources, and if the AI technology is being accessed by multiple parties.

Practical Steps to Avoid HIPAA Non-Compliance

With the risks and challenges of using PHI in AI technology in mind, here are several suggestions that Covered Entities and Business Associates can follow to help minimize the risk of non-compliance with HIPAA's rules when using PHI in AI technology:

Develop and Implement Policies and Procedures

Determine whether existing policies and procedures regarding the collection, handling, distribution, and use of PHI adequately cover the uses of PHI with AI technology. If not, then new policies should be developed and implemented that specifically address approved use cases of PHI in AI technology. For example, implement a policy that restricts employee use of PHI in unapproved AI technology for personal use, while granting the limited use of PHI in approved AI technology as part of the Covered Entity's or Business Associate's services.

- AI Governance – Determine whether an existing privacy and security governance team can adequately address the uses of PHI in AI technology. If not, consider creating a separate AI Governance team to provide continual oversight over the uses of AI technology.
- Update Contracts – Review and update contract templates and Business Associate Agreement templates and include additional language to address the risks associated with using PHI in AI technology.
- Training and Awareness – Update training to include uses of PHI in AI technology and the risks of HIPAA non-compliance when using AI technology.
- Code of Conduct – Develop a code of conduct with respect to the uses of PHI in AI technology and share the code of conduct with other Covered Entities and Business Associates whose data will be used by the AI technology.
- Transparency – Covered Entities should include the uses of PHI in their Notice of Privacy Practices, and Business Associates should develop materials to share with Covered Entities that outline their uses of PHI in AI technology.
- Risk Assessments – Conduct HIPAA risk assessments to identify risks to the integrity, confidentiality, and availability of PHI when used in AI technology. Assessments should be conducted regularly, especially when there are changes to existing processes or technology or with the development of new processes or technology.
- Expert Support – Seek out the support of experienced data privacy and security professionals to help understand the risks of using PHI in AI technology, and implement best practices to minimize risks to HIPAA non-compliance when using PHI in AI technology.

With the development and use of AI technology in healthcare, it is hard to imagine Covered Entities and Business Associates not adopting and using AI technology because of the potential benefits. However, there are several risks to HIPAA compliance that can impact the use of PHI in AI technology. Establishing a strong set of policies, protocols, governance, and monitoring processes will help Covered Entities and Business Associates safely minimize the risks involved with using PHI in AI technology.

Update for January 2023: NIST AI Risk Management Framework

The NIST AI Risk Management Framework (AI RMF) provides healthcare organizations with a structured way to evaluate and manage the risks of artificial intelligence while aligning with HIPAA's privacy and security standards. Unlike HIPAA, which sets baseline requirements for safeguarding Protected Health Information (PHI), the NIST framework focuses on principles such as validity, reliability, safety, security, explainability, privacy, and fairness in AI systems. For covered entities and business associates, this means that when deploying AI tools to process or analyze healthcare data, the AI RMF can be used alongside HIPAA to ensure not only regulatory compliance but also trustworthy and ethical AI practices. The framework is available as an overview on the NIST website.

Update for March 2025: HHS OCR Proposed Security Security Rule Update Has Impact on AI

and PHI

On January 6, 2025, the HHS Office for Civil Rights (OCR) proposed the first major update to the HIPAA Security Rule in 20 years, citing the rise in ransomware and the need for stronger cybersecurity. For organizations deploying artificial intelligence in healthcare, these changes are especially significant, as they remove the distinction between required and addressable safeguards and introduce stricter expectations for risk management, encryption, and resilience. AI systems that process Protected Health Information (PHI) will be subject to these enhanced standards, meaning vendors and covered entities must reassess their security controls and ensure compliance before integrating AI into clinical or administrative workflows.

Author: Todd L. Mayover, CIPP E/US, is an experienced in-house attorney, consultant and data privacy compliance expert with more than two decades of experience working on compliance, legal, privacy, and regulatory affairs issues for companies in the digital health, healthcare, life sciences and pharmaceutical sectors. At Privacy Aviator LLC, Todd provides guidance to early-stage and multinational companies on complex AI and data privacy compliance programs, focusing on AI, GDPR, HIPAA, HITECH, PIPL, and various other U.S. state and international AI and privacy laws and regulations. You connect with Todd directly via LinkedIn

- What is HIPAA Incident Management?
- What is a HIPAA Audit Checklist?
- HIPAA Risk Assessment

Get The FREE
HIPAA Compliance Checklist

Immediate Delivery of Checklist Link To Your Email Address

Work Email *

Get Free Checklist

Appendix J

Sarah Silverman, you can't be serious! You are suing a chatbot?? Be grateful you are not Mark Walters!!

I. Introduction

A rabbi, a priest and a chatbot walk into a bar. I don't know about you, but I would sure like to hear Sarah Silverman complete that story. I'm sure she will end it better than I, if I dare to complete it (stay tuned). Sarah Silverman, in case you don't know, is a brilliant comedian. A 21st century Mrs. Maisel. According to Kramer, she's got the "jimmy legs." Everything she says is funny. Well, almost everything. Recently she undertook a rather unfunny campaign; she is suing two chatbots. OK, technically she is not suing the chatbots; she is suing the companies behind the chatbots, OpenAI, Inc. and Meta Platforms, Inc. Sarah has some company in her lawsuit. She is joined by two authors, and hopes to spearhead a class action lawsuit against Meta and OpenAI.

Why would Sarah sue a chatbot? That is an excellent question. We can find the answer to that question by reading the complaint her attorneys filed in court. Sarah and her fellow plaintiffs do have something to complain about, if we believe her lawyers. Initially, Sarah's lawyers filed a lawsuit against ChatGPT on behalf of two other authors, Paul Tremblay and Mona Awad. Haven't heard of them? Neither have I. Ten days later, the same attorneys filed Sarah's lawsuit against Meta and OpenAI.

It doesn't hurt to have a celebrity plaintiff backing your cause. Celebrity defendants often add *cache* to a case. For example, Tom Brady is a defendant in a class-action lawsuit brought by people who feel that Tom's commercials hawking cryptocurrencies may have mislead them into unwise investments. These are some of the same people who reached out to Warren Buffet to coach their kids about football, because Tom was too busy doing crypto commercials. While Warren throws a pretty tight spiral, his coaching, nevertheless, left something to be desired. Rumor has it that some intense late night negotiations

between Warren's attorneys and those parents staved off a lawsuit against Warren for misrepresenting his football coaching skills.

Back to why Sarah sued a chatbot. According to her complaint, Meta did a couple of things wrong. First, to set the playing field level for the court, Sarah's attorneys define artificial intelligence. They tell us in paragraph 17 of the complaint that, "*Artificial intelligence* is commonly abbreviated 'AI.' AI software is designed to algorithmically simulate human reasoning or inference, often using statistical methods." There it is in two sentences, fifteen words: the definition of AI. Now that the court understands what AI is, Sarah's attorneys tell us what Meta did wrong in creating the monster chatbot LLaMA ("a set of large language models", or a sheep-like animal with a very long neck, just another software animal metaphor). According to Sarah's attorneys, some of Sarah's writings were fed to (the complaint says "ingested by") this LLaMA and are now stuck in its throat. And that is a problem for Meta.

According to the complaint, Meta committed these transgressions when it fed LLaMA Sarah's works:

1. It copied Sarah's works when it included them in LLaMA, without Sarah's permission;
2. It didn't pay Sarah when it included her works in LLaMA;
3. It creates "derivative works" based on Sarah's works when LLaMA creates its output;
4. It removed copyright notices from Sarah's works when it included those works in LLaMA; and
5. LLaMA is unfairly competing against Sarah when it does its thing.

I wonder what Meta will say? Will it ask LLaMA to format its answer to Sarah's complaint? Probably not based on the experience of Steven Schwartz, Esq., who used output from ChatGPT in court filings without checking if the output was real or an hallucination. Unfortunately for attorney Schwartz, ChatGPT was hallucinating at the time; its output bore no semblance to reality and the cases it cited were all fake cases. Adding insult to injury, the judge in the matter sanctioned attorney Schwartz, not ChatGPT, to the tune of a $5,000 penalty for presenting fraudulent cases to the court Perhaps attorney Schwartz might consider joining Sarah as a class-action plaintiff in her suit.

However, even without the benefit of output from LLaMA, we have an inkling of what Meta will say. The chances are that it will cite the federal copyright law of the United States and will cite real cases that have been decided by our courts interpreting those laws in the context of the Internet. And if this court decides in a manner consistent with prior court decisions, the chances are that Sarah's complaint will have a short shelf-life. If I were a betting person, I would wager $5 that Sarah's off-Broadway play, *The Bedwetter*, has a longer run in the theater than her complaint has in the courts.

II. Federal Copyright Law

To understand the strengths and weaknesses of Sarah's complaint, it is unfortunate but unavoidable that we must know a little bit about our federal copyright laws. Copyright law is the law that protects the rights of an author to prevent their works from being copied without their permission and / or without them receiving compensation. Our founding fathers considered copyright law to be very important. The first federal copyright statute was passed in 1790. Over time Congress has revised our copyright laws and the current version was enacted in 1976. The guts of our copyright law is found in a particular statute with the moniker 17 U.S.C §106. This statute grants to the authors of creative works certain exclusive rights, all of which center around the ability to copy and reproduce the creative work of an author. It is commonly said that the copyright statute grants a monopoly to authors to have the exclusive right to copy their works. Thanks to Mickey Mouse and Sonny Bono, that monopoly lasts for 70 years after the death of the author.

In order to claim that a defendant is violating an author's copyright rights, an author must first prove that the defendant has copied his/her work. Unless the plaintiff can demonstrate that, the plaintiff has no case.

Because life is complicated, a copyright infringement case does not end with the plaintiff proving that a defendant has unlawfully copied the plaintiff's work. The defendant then gets an opportunity to explain that even though it copied the plaintiff's work, its copying is justified under the doctrine of "fair use." Fair use is the copyright equivalent of the "get-out-of-jail-free" card in the game of

Monopoly. Every defendant who has ever been caught red-handed copying a plaintiff's work pleads fair use to justify their copying. The legal nuts and bolts of fair use are found right after Section 106 in 17 U.S.C. §107.

Luckily for lawyers, fair use is a nebulous concept which means clients have to spend lots of money on legal fees when fair use considered by a court. Courts have explained the fair use doctrine this way: This exception "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." 17 U.S.C. §107 describes four factors a court may consider to determine if a defendant's copying is protected by fair use. Those factors are:

> "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work."

As we shall see, those four factors spell doom for Sarah's complaint.

III. Applying Copyright Law to Sarah's Complaint

A. Did Meta Copy Sarah's Works?

When we review the list of Sarah's grievances, only one states that Meta copied Sarah's work without her permission. But a closer read of Sarah's complaint doesn't allege that Meta actually copied Sarah's works. It says that Meta may have obtained Sarah's works (her lawyers aren't certain) from publicly available repositories of books. Whether these repositories had permission to copy the original books is another story. Sarah's lawyers suggest they did not have permission. However this gap in the chain of custody begs a central question: if the repositories are the copyright thieves, why aren't the repositories named as defendants in the complaint? Which goes back to a conundrum law school students are asked to solve in their first year property class in law school. If a

person buys property from a vendor who has stolen the property from its true owner, is the buyer liable to the true owner? To find out the answer, one must shell out hundreds of thousands of dollars and devote three years of their life to law school.

B. Was Meta's Use of Sarah's Works a "Fair Use"?

If Sarah convinces the court that Meta did, in fact, copy her works without her permission, then she has to fight the battle that Meta's use of her work is not fair use. And that is going to be an even harder fight to win.

The Internet has been around a while. Long enough that even our courts have decided cases involving Internet disputes. Long enough that lawyers can now say that certain legal principles are "well-settled." And the fair use of copyrighted material on the Internet is one of those well-settled principles.

For example, in 2002, in the case of Kelly v. Ariba Soft Corporation, the Ninth Circuit Court of Appeals was asked to decide if a search engine could use photographs owned by the plaintiff, Kelly, without his approval, if those photographs were presented as thumbnail (miniature) images. The images were identical to Kelly's pictures, just a lot smaller. Kelly did not give Ariba permission to use his pictures; Ariba gave no attribution to Kelly; Ariba did not pay Kelly. Clearly Kelly's pictures were copied when Ariba stored them and displayed them on a user's screen. ***Verdict: for the defendant. Reason: Ariba's use of Kelly's pictures was a fair use*** of his copyrighted work; therefore Kelly's rights were not infringed by Ariba. One of the key issues in a fair use analysis is the concept of transformative use. A use is transformative if the original work is transformed by the defendant in such a manner as to create a new work. The more transformative the new work is, the more likely the use is a fair use. Another key concept in a fair use analysis is the economic impact of the infringer's activity on the author. If the infringer's use of the work deprives the author of income, then the infringer's use will not be deemed fair use. In Ariba, the court held that Ariba had substantially transformed Kelly's pictures by miniaturizing them. Further it found that Ariba's use of Kelly's works had no financial impact on Kelly, and if anything, may drive business Kelly's way. So for those reasons the court held that

while Ariba Soft copied Kelly's pictures without his authorization, Ariba Soft's use of the pictures was a fair use and did not violate federal copyright law.

Of course any history of the Internet cannot be told without including a chapter about those twin titans of Internet commerce: Google and pornography. After the Kelly case, the fair use doctrine was again tested in 2007 in the case of Perfect 10, Inc. v. Google. Perfect 10 was a publisher of pornographic images. (Who can forget Bo Derek in 10?). Perfect 10 sued Google claiming that Google's Internet browser was infringing its copyrighted images when it included those images as thumbnail images in Google's browser results. Déjà vu all over again? Pretty much yes. The Ninth Circuit held, once again, that publishing a thumbnail of an image was a transformative use of the original image, thus protected by the fair use doctrine. Further it held that Perfect 10's damages were speculative (again Google was probably driving traffic to Perfect 10's web site; you try twerking to a thumbnail of Bo Derek!) and therefore did not support a claim of copyright infringement.

The final nail in Sarah's coffin of fair use may have been struck in the 2015 case of Author's Guild v Google. In that case the Author's Guild sued Google when Google created a repository of books that was searchable online. Google, doing no harm, never obtained the consent of the publishers and authors of those books to include them in the repository, nor did it pay them. When a particular book is retrieved from Google's data base by a user's search, portions of the book are reproduced for the user's viewing *ver batim*. ***Verdict: for the defendant. Reason: Google's use of the original books was transformative***. If reproducing portions of copyrighted works *ver batim* over the Internet without the author's permission is fair use, it is hard to conceive what isn't fair use on the Internet. The court justified its holding primarily focusing on the economic impact of Google's use of the books on the books' authors, and noted that if anything, Google's use of the books may create sales for the authors, supplementing their income.

With such legal precedent, it is hard to see Sarah winning her case against Meta. Meta is not reproducing Sarah's works when LLaMA speaks. LLaMA may use Sarah's works as data to create its output, but its output is not a reproduction of Sarah's copyrighted works. So where is the copying? Its output is highly transformative. If courts have held that replication of an exact image, but

miniaturized, is transformative, then certainly a new work that is different from an original work will be considered transformative. And what are Sarah's damages? Is she maintaining that her audience is now getting its laughs from a LLaMA instead of seeing her perform and instead of going to *The Bedwetter*? It would appear so. When she complains that LLaMA engages in unfair competition, I guess she is conceding that LLaMA's output is qualitatively equal and competitive with her output. And that LLaMA is siphoning off her audience and sales of her works.

Sarah, lighten up! For gosh sakes be grateful you are not Mark Walters!

IV. Who is Mark Walters? Is he funny like Sarah? What's his Beef?

Here is what we know about Mark Walters. He is a "natural person." He resides in Georgia. That's all we know about who Mark Walters is. However, we know a lot more about who Mark Walters is not. Mark Walters is not:

- The treasurer and chief financial officer of the Second Amendment Foundation ("SAF")
- Someone who steals from the SAF
- Someone who after stealing funds from the SAF then engages in conspiratorial activity to conceal his theft of funds
- Someone who has been sued by Alan Gottlieb, the founder of the SAF for doing those things we now know Mr. Walters did not do

We know much more about who Mr. Walters is not than who he is courtesy of ChatGPT. ChatGPT made the mistake of writing that Mr. Walters is the person who he claims not to be. That is, in response to a prompt from Fred Riehl, a reporter, ChatGPT spilled the aforementioned alleged beans on Mr. Walters, except the beans contained no kernel of truth. ChatGPT was hallucinating again. And again and again, because when Mr. Riehl asked ChatGPT if it was sure that Mr. Walters was the perpetrator of these dastardly deeds, and asked it to produce a copy of a complaint filed in court describing Mr. Walter's allegedly

dastardly deeds, ChatGPT was more than happy to comply and produced a fictitious complaint filed in court (Steven Schwartz, Esq. are you listening?).

When Mr. Riehl contacted the real Mr. Walters and showed him the lies ChatGPT was spewing, Mr. Walters was not amused. In fact he sued ChatGPT's creator and owner, OpenAI, LLC. Here is a copy of *his* complaint.

Mr. Walters sued OpenAI not for copyright infringement like Sarah sued Meta for. Instead, Mr. Walters sued OpenAI for defamation. Mr. Walter's complaint doesn't really tell us what law OpenAI violated, but it sure sounds like defamation. After all it can't be good for Mr. Walters' reputation for a chatbot to be spreading these rumors about him. Would you hire a person like Mr. Walters if he did what ChatGPT said he did?

Thanks to Johnny Depp and Amber Heard we are all experts in defamation lawsuits. To prevail in a defamation trial, a plaintiff, like Mr. Walters, has to prove two things. First that he was defamed by the defendant. Second that the defendant's defamation caused him economic harm which can then be recovered from the defendant. Part one seems like a slam dunk. ChatGPT was spewing false statements about Mr. Walters like there was no tomorrow. Further when it was asked to verify the truth of its false statements, ChatGPT continued to make up crap about Mr. Walters. Not one of ChatGPT's finer moments.

But what about part two? What are Mr. Walter's damages? Can he prove that the statements ChatGPT made to Fred Riehl caused him any economic harm? Did Fred Riehl withhold money from Mr. Walter's based on ChatGPT's statements? Not according to his complaint. Damages are a sticking point for many potential plaintiffs in defamation lawsuits. It is one thing to claim that a defendant defamed you; it is quite another to prove the such defamation led to your economic demise. For better or for worse depending on your perspective, we are not all Johnny Depp, and when someone says something bad about us, we can't claim that Disney broke its contract with us because of the defendant's defamatory statements.

Mr. Walter's attorney appears cognizant of this roadblock. In paragraph 32 of his complaint Mr. Walters alleges that the statements made by ChatGPT were "false and malicious." Really? Can a chatbot write a statement with malice? Is Mr.

Walters and his attorney perhaps getting a bit anthropomorphic here? Or perhaps Mr. Walters and his attorney are simply applying the lessons learned from the movie *Absence of Malice*, hoping that a showing of malice will lessen the need to show real economic harm.

Good luck to Mr. Walters. I would share his sense of outrage if a chatbot said about me what it said about him. But that doesn't necessarily mean I would win a lawsuit.

When you compare Sarah's complaint with the complaint of Mr. Walters, it sure seems like Mr. Walters is getting the short end of the stick. Sarah should be grateful that while her work may have been "ingested" by a chatbot, they were not spewed forth in a defaming hallucinatory rant. We all need to look on the bright side of things.

V. What about that Joke?

What about that opening line to the joke at the top of the article: "a rabbi, a priest and a chatbot walk into a bar"? I asked ChatGPT to complete the joke. Here was its first response:

> ...and the bartender says, "Is this some kind of interfaith support group, or are you all just here to ask me for the meaning of life?" The chatbot replies, "Actually, I already know the answer is 42, but I'm just here to learn some human humor!"

Sort of mildly funny in a bland way. In case you are not familiar with it, the snippet of the meaning of life being 42 comes from Douglas Adams' *Hitchhiker's Guide to the Galaxy*.

Wondering if ChatGPT might improve with practice, I asked it to complete the joke again. It second response was:

> ... and the bartender says, "Is this a setup for a punchline or just the start of an unusual support group?"

My take was that ChatGPT had moved on to more pressing topics.

Here is my attempt at a punchline:

> The rabbi says to the chatbot, "If you are Jewish come with me and I will have you circumcised." The priest says to the chatbot, "If you are Catholic, come with me and I will conduct confession." After hallucinating for a moment, the chatbot says, "I will go with the rabbi. I confess I have nothing to lose."

Sarah, please help!

Postscript: *As predicted, most of Sarah's lawsuit was dismissed by the district court in late November. Sarah's lawsuit was filed on July 7, 2023, and dismissed on November 21, 2023, thus having a shelf-life of a little more than 4 months. The Bedwetter had a run of approximately two months. I lost my $5 bet.*

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 512 **July 29, 2024**

Generative Artificial Intelligence Tools

To ensure clients are protected, lawyers using generative artificial intelligence tools must fully consider their applicable ethical obligations, including their duties to provide competent legal representation, to protect client information, to communicate with clients, to supervise their employees and agents, to advance only meritorious claims and contentions, to ensure candor toward the tribunal, and to charge reasonable fees.

I. Introduction

Many lawyers use artificial intelligence (AI) based technologies in their practices to improve the efficiency and quality of legal services to clients.[1] A well-known use is electronic discovery in litigation, in which lawyers use technology-assisted review to categorize vast quantities of documents as responsive or non-responsive and to segregate privileged documents. Another common use is contract analytics, which lawyers use to conduct due diligence in connection with mergers and acquisitions and large corporate transactions. In the realm of analytics, AI also can help lawyers predict how judges might rule on a legal question based on data about the judge's rulings; discover the summary judgment grant rate for every federal district judge; or evaluate how parties and lawyers may behave in current litigation based on their past conduct in similar litigation. And for basic legal research, AI may enhance lawyers' search results.

This opinion discusses a subset of AI technology that has more recently drawn the attention of the legal profession and the world at large – generative AI (GAI), which can create various types of new content, including text, images, audio, video, and software code in response to a user's prompts and questions.[2] GAI tools that produce new text are prediction tools that generate a statistically probable output when prompted. To accomplish this, these tools analyze large amounts of digital text culled from the internet or proprietary data sources. Some GAI tools are described as "self-learning," meaning they will learn from themselves as they cull more data. GAI tools may assist lawyers in tasks such as legal research, contract review, due diligence, document review, regulatory compliance, and drafting letters, contracts, briefs, and other legal documents.

[1] There is no single definition of artificial intelligence. At its essence, AI involves computer technology, software, and systems that perform tasks traditionally requiring human intelligence. The ability of a computer or computer-controlled robot to perform tasks commonly associated with intelligent beings is one definition. The term is frequently applied to the project of developing systems that appear to employ or replicate intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience. BRITTANICA, https://www.britannica.com/technology/artificial-intelligence (last visited July 12, 2024).

[2] George Lawton, *What is Generative AI? Everything You Need to Know*, TECHTARGET (July 12, 2024), https://www.techtarget.com/searchenterpriseai/definition/generative-AI.

GAI tools—whether general purpose or designed specifically for the practice of law—raise important questions under the ABA Model Rules of Professional Conduct.[3] What level of competency should lawyers acquire regarding a GAI tool? How can lawyers satisfy their duty of confidentiality when using a GAI tool that requires input of information relating to a representation? When must lawyers disclose their use of a GAI tool to clients? What level of review of a GAI tool's process or output is necessary? What constitutes a reasonable fee or expense when lawyers use a GAI tool to provide legal services to clients?

At the same time, as with many new technologies, GAI tools are a moving target—indeed, a *rapidly* moving target—in the sense that their precise features and utility to law practice are quickly changing and will continue to change in ways that may be difficult or impossible to anticipate. This Opinion identifies some ethical issues involving the use of GAI tools and offers general guidance for lawyers attempting to navigate this emerging landscape.[4] It is anticipated that this Committee and state and local bar association ethics committees will likely offer updated guidance on professional conduct issues relevant to specific GAI tools as they develop.

II. Discussion

A. Competence

Model Rule 1.1 obligates lawyers to provide competent representation to clients.[5] This duty requires lawyers to exercise the "legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation," as well as to understand "the benefits and risks associated" with the technologies used to deliver legal services to clients.[6] Lawyers may ordinarily achieve the requisite level of competency by engaging in self-study, associating with another competent lawyer, or consulting with an individual who has sufficient expertise in the relevant field.[7]

To competently use a GAI tool in a client representation, lawyers need not become GAI experts. Rather, lawyers must have a reasonable understanding of the capabilities and limitations

---

[3] Many of the professional responsibility concerns that arise with GAI tools are similar to the issues that exist with other AI tools and should be considered by lawyers using such technology.

[4] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2023. The Opinion addresses several imminent ethics issues associated with the use of GAI, but additional issues may surface, including those found in Model Rule 7.1 ("Communications Concerning a Lawyer's Services"), Model Rule 1.7 ("Conflict of Interest: Current Clients"), and Model Rule 1.9 ("Duties to Former Clients"). *See, e.g.*, Fla. State Bar Ass'n, Prof'l Ethics Comm. Op. 24-1, at 7 (2024) (discussing the use of GAI chatbots under Florida Rule 4-7.13, which prohibits misleading content and unduly manipulative or intrusive advertisements); Pa. State Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. & Philadelphia Bar Ass'n Prof'l Guidance Comm. Joint Formal Op. 2024-200 [hereinafter Pa. & Philadelphia Joint Formal Opinion 2024-200], at 10 (2024) ("Because the large language models used in generative AI continue to develop, some without safeguards similar to those already in use in law offices, such as ethical walls, they may run afoul of Rules 1.7 and 1.9 by using the information developed from one representation to inform another."). Accordingly, lawyers should consider all rules before using GAI tools.

[5] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2023) [hereinafter MODEL RULES].

[6] MODEL RULES R. 1.1 & cmt. [8]. *See also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 2–3 (2017) [hereinafter ABA Formal Op. 477R] (discussing the ABA's "technology amendments" made to the Model Rules in 2012).

[7] MODEL RULES R. 1.1 cmts. [1], [2] & [4]; Cal. St. Bar, Comm. Prof'l Resp. Op. 2015-193, 2015 WL 4152025, at *2–3 (2015).

of the specific GAI technology that the lawyer might use. This means that lawyers should either acquire a reasonable understanding of the benefits and risks of the GAI tools that they employ in their practices or draw on the expertise of others who can provide guidance about the relevant GAI tool's capabilities and limitations.[8] This is not a static undertaking. Given the fast-paced evolution of GAI tools, technological competence presupposes that lawyers remain vigilant about the tools' benefits and risks.[9] Although there is no single right way to keep up with GAI developments, lawyers should consider reading about GAI tools targeted at the legal profession, attending relevant continuing legal education programs, and, as noted above, consulting others who are proficient in GAI technology.[10]

With the ability to quickly create new, seemingly human-crafted content in response to user prompts, GAI tools offer lawyers the potential to increase the efficiency and quality of their legal services to clients. Lawyers must recognize inherent risks, however.[11] One example is the risk of producing inaccurate output, which can occur in several ways. The large language models underlying GAI tools use complex algorithms to create fluent text, yet GAI tools are only as good as their data and related infrastructure. If the quality, breadth, and sources of the underlying data on which a GAI tool is trained are limited or outdated or reflect biased content, the tool might produce unreliable, incomplete, or discriminatory results. In addition, the GAI tools lack the ability to understand the meaning of the text they generate or evaluate its context.[12] Thus, they may combine otherwise accurate information in unexpected ways to yield false or inaccurate results.[13] Some GAI tools are also prone to "hallucinations," providing ostensibly plausible responses that have no basis in fact or reality.[14]

Because GAI tools are subject to mistakes, lawyers' uncritical reliance on content created by a GAI tool can result in inaccurate legal advice to clients or misleading representations to courts and third parties. Therefore, a lawyer's reliance on, or submission of, a GAI tool's output—without

---

[8] Pa. Bar Ass'n, Comm. on Legal Ethics & Prof'l Resp. Op. 2020-300, 2020 WL 2544268, at *2–3 (2020). *See also* Cal. State Bar, Standing Comm. on Prof'l Resp. & Conduct Op. 2023-208, 2023 WL 4035467, at *2 (2023) adopting a "reasonable efforts standard" and "fact-specific approach" to a lawyer's duty of technology competence, citing ABA Formal Opinion 477R, at 4).

[9] *See* New York County Lawyers Ass'n Prof'l Ethics Comm. Op. 749 (2017) (emphasizing that "[l]awyers must be responsive to technological developments as they become integrated into the practice of law"); Cal. St. Bar, Comm. Prof'l Resp. Op. 2015-193, 2015 WL 4152025, at *1 (2015) (discussing the level of competence required for lawyers to handle e-discovery issues in litigation).

[10] MODEL RULES R. 1.1 cmt. [8]; *see* Melinda J. Bentley, *The Ethical Implications of Technology in Your Law Practice: Understanding the Rules of Professional Conduct Can Prevent Potential Problems*, 76 J. MO. BAR 1 (2020) (identifying ways for lawyers to acquire technology competence skills).

[11] As further detailed in this opinion, lawyers' use of GAI raises confidentiality concerns under Model Rule 1.6 due to the risk of disclosure of, or unauthorized access to, client information. GAI also poses complex issues relating to ownership and potential infringement of intellectual property rights and even potential data security threats.

[12] *See,* W. Bradley Wendel, *The Promise and Limitations of AI in the Practice of Law,* 72 OKLA. L. REV. 21, 26 (2019) (discussing the limitations of AI based on an essential function of lawyers, making normative judgments that are impossible for AI).

[13] *See, e.g.*, Karen Weise & Cade Metz, *When A.I. Chatbots Hallucinate*, N.Y. TIMES (May 1, 2023).

[14] Ivan Moreno, *AI Practices Law 'At the Speed of Machines.' Is it Worth It?*, LAW360 (June 7, 2023); *See* Varun Magesh, Faiz Surani, Matthew Dahl, Mirac Suzgun, Christopher D. Manning, & Daniel E. Ho, *Hallucination Free? Assessing the Reliability of Leading AI Legal Research Tools*, STANFORD UNIVERSITY (June 26, 2024), *available at* https://dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf (study finding leading legal research companies' GAI systems "hallucinate between 17% and 33% of the time").

an appropriate degree of independent verification or review of its output—could violate the duty to provide competent representation as required by Model Rule 1.1.[15] While GAI tools may be able to significantly assist lawyers in serving clients, they cannot replace the judgment and experience necessary for lawyers to competently advise clients about their legal matters or to craft the legal documents or arguments required to carry out representations.

The appropriate amount of independent verification or review required to satisfy Rule 1.1 will necessarily depend on the GAI tool and the specific task that it performs as part of the lawyer's representation of a client. For example, if a lawyer relies on a GAI tool to review and summarize numerous, lengthy contracts, the lawyer would not necessarily have to manually review the entire set of documents to verify the results if the lawyer had previously tested the accuracy of the tool on a smaller subset of documents by manually reviewing those documents, comparing then to the summaries produced by the tool, and finding the summaries accurate. Moreover, a lawyer's use of a GAI tool designed specifically for the practice of law or to perform a discrete legal task, such as generating ideas, may require less independent verification or review, particularly where a lawyer's prior experience with the GAI tool provides a reasonable basis for relying on its results.

While GAI may be used as a springboard or foundation for legal work—for example, by generating an analysis on which a lawyer bases legal advice, or by generating a draft from which a lawyer produces a legal document—lawyers may not abdicate their responsibilities by relying solely on a GAI tool to perform tasks that call for the exercise of professional judgment. For example, lawyers may not leave it to GAI tools alone to offer legal advice to clients, negotiate clients' claims, or perform other functions that require a lawyer's personal judgment or participation.[16] Competent representation presupposes that lawyers will exercise the requisite level of skill and judgment regarding all legal work. In short, regardless of the level of review the lawyer selects, the lawyer is fully responsible for the work on behalf of the client.

Emerging technologies may provide an output that is of distinctively higher quality than current GAI tools produce, or may enable lawyers to perform work markedly faster and more economically, eventually becoming ubiquitous in legal practice and establishing conventional expectations regarding lawyers' duty of competence.[17] Over time, other new technologies have become integrated into conventional legal practice in this manner.[18] For example, "a lawyer would have difficulty providing competent legal services in today's environment without knowing how

---

[15] *See generally* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451, at 1 (2008) [hereinafter ABA Formal Op. 08-451] (concluding that "[a] lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under Model Rule 1.1").

[16] *See* Fla. State Bar Ass'n, Prof'l Ethics Comm. Op. 24-1, *supra* note 4.

[17] *See, e.g.*, Sharon Bradley, *Rule 1.1 Duty of Competency and Internet Research: Benefits and Risks Associated with Relevant Technology* at 7 (2019), *available at* https://ssrn.com/abstract=3485055 ("View Model Rule 1.1 as elastic. It is expanding as legal technology solutions expand. The ever-changing shape of this rule makes clear that a lawyer cannot simply learn technology today and never again update their skills or knowledge.").

[18] *See, e.g.*, Smith v. Lewis, 530 P.2d 589, 595 (Cal. 1975) (stating that a lawyer is expected "to possess knowledge of those plain and elementary principles of law which are commonly known by well-informed attorneys, and to discover those additional rules of law which, although not commonly known, may readily be found by *standard research techniques*") (emphasis added); Hagopian v. Justice Admin. Comm'n, 18 So. 3d 625, 642 (Fla. Dist. Ct. App. 2009) (observing that lawyers have "become expected to use computer-assisted legal research to ensure that their research is complete and up-to-date, but the costs of this service can be significant").

to use email or create an electronic document."[19] Similar claims might be made about other tools such as computerized legal research or internet searches.[20] As GAI tools continue to develop and become more widely available, it is conceivable that lawyers will eventually have to use them to competently complete certain tasks for clients.[21] But even in the absence of an expectation for lawyers to use GAI tools as a matter of course,[22] lawyers should become aware of the GAI tools relevant to their work so that they can make an informed decision, as a matter of professional judgment, whether to avail themselves of these tools or to conduct their work by other means.[23] As previously noted regarding the possibility of outsourcing certain work, "[t]here is no unique blueprint for the provision of competent legal services. Different lawyers may perform the same tasks through different means, all with the necessary 'legal knowledge, skill, thoroughness and preparation.'"[24] Ultimately, any informed decision about whether to employ a GAI tool must consider the client's interests and objectives.[25]

---

[19] ABA Formal Op. 477R, *supra* note 6, at 3 (quoting ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012)).

[20] *See, e.g.*, Bradley, *supra* note 17, at 3 ("Today no competent lawyer would rely solely upon a typewriter to draft a contract, brief, or memo. Typewriters are no longer part of 'methods and procedures' used by competent lawyers."); Lawrence Duncan MacLachlan, *Gandy Dancers on the Web: How the Internet Has Raised the Bar on Lawyers' Professional Responsibility to Research and Know the Law*, 13 GEO. J. LEGAL ETHICS 607, 608 (2000) ("The lawyer in the twenty-first century who does not effectively use the Internet for legal research may fall short of the minimal standards of professional competence and be potentially liable for malpractice"); Ellie Margolis, *Surfin' Safari—Why Competent Lawyers Should Research on the Web*, 10 YALE J.L. & TECH. 82, 110 (2007) ("While a lawyer's research methods reveal a great deal about the competence of the research, the method of research is ultimately a secondary inquiry, only engaged in when the results of that research process is judged inadequate. A lawyer who provides the court with adequate controlling authority is not going to be judged incompetent whether she found that authority in print, electronically, or by any other means."); Michael Thomas Murphy, *The Search for Clarity in an Attorney's Duty to Google*, 18 LEGAL COMM. & RHETORIC: JALWD 133, 133 (2021) ("This Duty to Google contemplates that certain readily available information on the public Internet about a legal matter is so easily accessible that it must be discovered, collected, and examined by an attorney, or else that attorney is acting unethically, committing malpractice, or both"); Michael Whiteman, *The Impact of the Internet and Other Electronic Sources on an Attorney's Duty of Competence Under the Rules of Professional Conduct*, 11 ALB. L.J. SCI. & TECH. 89, 91 (2000) ("Unless it can be shown that the use of electronic sources in legal research has become a standard technique, then lawyers who fail to use electronic sources will not be deemed unethical or negligent in his or her failure to use such tools.").

[21] *See* MODEL RULES R. 1.1 cmt. [5] (stating that "[c]ompetent handling of a particular matter includes . . . [the] use of methods and procedures meeting the standards of competent practitioners"); New York County Lawyers Ass'n Prof'l Ethics Comm. Op. 749, 2017 WL 11659554, at *3 (2017) (explaining that the duty of competence covers not only substantive knowledge in different areas of the law, but also the manner in which lawyers provide legal services to clients).

[22] The establishment of such an expectation would likely require an increased acceptance of GAI tools across the legal profession, a track record of reliable results from those platforms, the widespread availability of these technologies to lawyers from a cost or financial standpoint, and robust client demand for GAI tools as an efficiency or cost-cutting measure.

[23] Model Rule 1.5's prohibition on unreasonable fees, as well as market forces, may influence lawyers to use new technology in favor of slower or less efficient methods.

[24] ABA Formal Op. 08-451, *supra* note 15, at 2. *See also id.* ("Rule 1.1 does not require that tasks be accomplished in any special way. The rule requires only that the lawyer who is responsible to the client satisfies her obligation to render legal services competently.").

[25] MODEL RULES R. 1.2(a).

B. Confidentiality

A lawyer using GAI must be cognizant of the duty under Model Rule 1.6 to keep confidential all information relating to the representation of a client, regardless of its source, unless the client gives informed consent, disclosure is impliedly authorized to carry out the representation, or disclosure is permitted by an exception.[26] Model Rules 1.9(c) and 1.18(b) require lawyers to extend similar protections to former and prospective clients' information. Lawyers also must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[27]

Generally, the nature and extent of the risk that information relating to a representation may be revealed depends on the facts. In considering whether information relating to any representation is adequately protected, lawyers must assess the likelihood of disclosure and unauthorized access, the sensitivity of the information,[28] the difficulty of implementing safeguards, and the extent to which safeguards negatively impact the lawyer's ability to represent the client.[29]

Before lawyers input information relating to the representation of a client into a GAI tool, they must evaluate the risks that the information will be disclosed to or accessed by others outside the firm. Lawyers must also evaluate the risk that the information will be disclosed to or accessed by others *inside* the firm who will not adequately protect the information from improper disclosure or use[30] because, for example, they are unaware of the source of the information and that it originated with a client of the firm. Because GAI tools now available differ in their ability to ensure that information relating to the representation is protected from impermissible disclosure and access, this risk analysis will be fact-driven and depend on the client, the matter, the task, and the GAI tool used to perform it.[31]

Self-learning GAI tools into which lawyers input information relating to the representation, by their very nature, raise the risk that information relating to one client's representation may be disclosed improperly,[32] even if the tool is used exclusively by lawyers at the same firm.[33] This can occur when information relating to one client's representation is input into the tool, then later revealed in response to prompts by lawyers working on other matters, who then share that output with other clients, file it with the court, or otherwise disclose it. In other words, the self-learning

---

[26] MODEL RULES R. 1.6; MODEL RULES R. 1.6 cmt. [3].
[27] MODEL RULES R. 1.6(c).
[28] ABA Formal Op. 477R, *supra* note 6, at 1 (A lawyer "may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when … the nature of the information requires a higher degree of security.").
[29] MODEL RULES R. 1.6, cmt. [18].
[30] *See* MODEL RULES R. 1.8(b), which prohibits use of information relating to the representation of a client to the disadvantage of the client.
[31] *See* ABA Formal Op. 477R, *supra* note 6, at 4 (rejecting specific security measures to protect information relating to a client's representation and advising lawyers to adopt a fact-specific approach to data security).
[32] *See generally* State Bar of Cal. Standing Comm. on Prof'l Resp. & Conduct, PRACTICAL GUIDANCE FOR THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN THE PRACTICE OF LAW (2024), *available at* https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf; Fla. State Bar Ass'n, Prof'l Ethics Comm. Op. 24-1, *supra* note 4.
[33] *See* Pa. & Philadelphia Joint Formal Opinion 2024-200, *supra* note 4, at 10 (noting risk that information relating to one representation may be used to inform work on another representation).

GAI tool may disclose information relating to the representation to persons outside the firm who are using the same GAI tool. Similarly, it may disclose information relating to the representation to persons in the firm (1) who either are prohibited from access to said information because of an ethical wall or (2) who could inadvertently use the information from one client to help another client, not understanding that the lawyer is revealing client confidences. Accordingly, because many of today's self-learning GAI tools are designed so that their output could lead directly or indirectly to the disclosure of information relating to the representation of a client, a client's informed consent is required prior to inputting information relating to the representation into such a GAI tool.[34]

When consent is required, it must be informed. For the consent to be informed, the client must have the lawyer's best judgment about why the GAI tool is being used, the extent of and specific information about the risk, including particulars about the kinds of client information that will be disclosed, the ways in which others might use the information against the client's interests, and a clear explanation of the GAI tool's benefits to the representation. Part of informed consent requires the lawyer to explain the extent of the risk that later users or beneficiaries of the GAI tool will have access to information relating to the representation. To obtain informed consent when using a GAI tool, merely adding general, boiler-plate provisions to engagement letters purporting to authorize the lawyer to use GAI is not sufficient.[35]

Because of the uncertainty surrounding GAI tools' ability to protect such information and the uncertainty about what happens to information both at input and output, it will be difficult to evaluate the risk that information relating to the representation will either be disclosed to or accessed by others inside the firm to whom it should not be disclosed as well as others outside the firm.[36] As a baseline, all lawyers should read and understand the Terms of Use, privacy policy, and related contractual terms and policies of any GAI tool they use to learn who has access to the information that the lawyer inputs into the tool or consult with a colleague or external expert who has read and analyzed those terms and policies.[37] Lawyers may need to consult with IT professionals or cyber security experts to fully understand these terms and policies as well as the manner in which GAI tools utilize information.

Today, there are uses of self-learning GAI tools in connection with a legal representation when client informed consent is not required because the lawyer will not be inputting information relating to the representation. As an example, if a lawyer is using the tool for idea generation in a manner that does not require inputting information relating to the representation, client informed consent would not be necessary.

---

[34] This conclusion is based on the risks and capabilities of GAI tools as of the publication of this opinion. As the technology develops, the risks may change in ways that would alter our conclusion. *See* Fla. State Bar Ass'n, Prof'l Ethics Comm. Op. 24-1, *supra* note 4, at 2; W. Va. Lawyer Disciplinary Bd. Op. 24-01 (2024), *available at* http://www.wvodc.org/pdf/AILEO24-01.pdf.

[35] *See* W. Va. Lawyer Disciplinary Bd. Op. 24-01, *supra* note 34.

[36] Magesh et al. *supra* note 14, at 23 (describing some of the GAI tools available to lawyers as "difficult for lawyers to assess when it is safe to trust them. Official documentation does not clearly illustrate what they can do for lawyers and in which areas lawyers should exercise caution.")

[37] Stephanie Pacheco, *Three Considerations for Attorneys Using Generative AI,* BLOOMBERG LAW ANALYSIS (June 16, 2023, 4:00 pm), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-three-considerations-for-attorneys-using-generative-ai?context=search&index=7.

C. Communication

Where Model Rule 1.6 does not require disclosure and informed consent, the lawyer must separately consider whether other Model Rules, particularly Model Rule 1.4, require disclosing the use of a GAI tool in the representation.

Model Rule 1.4, which addresses lawyers' duty to communicate with their clients, 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."[38] Of particular relevance, 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." Additionally, Model Rule 1.4(b) obligates lawyers to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Comment [5] to Rule 1.4 explains, "the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation." Considering these underlying principles, questions arise regarding whether and when lawyers might be required to disclose their use of GAI tools to clients pursuant to Rule 1.4.

The facts of each case will determine whether Model Rule 1.4 requires lawyers to disclose their GAI practices to clients or obtain their informed consent to use a particular GAI tool. Depending on the circumstances, client disclosure may be unnecessary.

Of course, lawyers must disclose their GAI practices if asked by a client how they conducted their work, or whether GAI technologies were employed in doing so, or if the client expressly requires disclosure under the terms of the engagement agreement or the client's outside counsel guidelines.[39] There are also situations where Model Rule 1.4 requires lawyers to discuss their use of GAI tools unprompted by the client.[40] For example, as discussed in the previous section, clients would need to be informed in advance, and to give informed consent, if the lawyer proposes to input information relating to the representation into the GAI tool.[41] Lawyers must also consult clients when the use of a GAI tool is relevant to the basis or reasonableness of a lawyer's fee.[42]

Client consultation about the use of a GAI tool is also necessary when its output will influence a significant decision in the representation,[43] such as when a lawyer relies on GAI

---

[38] Baker v. Humphrey, 101 U.S. 494, 500 (1879).

[39] *See, e.g.*, MODEL RULES R. 1.4(a)(4) ("A lawyer shall . . . promptly comply with reasonable requests for information[.]").

[40] *See* MODEL RULES R. 1.4(a)(1) (requiring lawyers to "promptly inform the client of any decision or circumstance with respect to which the client's informed consent" is required by the rules of professional conduct).

[41] See section B for a discussion of confidentiality issues under Rule 1.6.

[42] See section F for a discussion of fee issues under Rule 1.5.

[43] Guidance may be found in ethics opinions requiring lawyers to disclose their use of temporary lawyers whose involvement is significant or otherwise material to the representation. *See, e.g.*, Va. State Bar Legal Ethics Op. 1850, 2010 WL 5545407, at *5 (2010) (acknowledging that "[t]here is little purpose to informing a client every time a lawyer outsources legal support services that are truly tangential, clerical, or administrative in nature, or even when basic legal research or writing is outsourced without any client confidences being revealed"); Cal. State Bar, Standing Comm. on Prof'l Resp. & Conduct Op. 2004-165, 2004 WL 3079030, at *2–3 (2004) (opining that a

technology to evaluate potential litigation outcomes or jury selection. A client would reasonably want to know whether, in providing advice or making important decisions about how to carry out the representation, the lawyer is exercising independent judgment or, in the alternative, is deferring to the output of a GAI tool. Or there may be situations where a client retains a lawyer based on the lawyer's particular skill and judgment, when the use of a GAI tool, without the client's knowledge, would violate the terms of the engagement agreement or the client's reasonable expectations regarding how the lawyer intends to accomplish the objectives of the representation.

It is not possible to catalogue every situation in which lawyers must inform clients about their use of GAI. Again, lawyers should consider whether the specific circumstances warrant client consultation about the use of a GAI tool, including the client's needs and expectations, the scope of the representation, and the sensitivity of the information involved. Potentially relevant considerations include the GAI tool's importance to a particular task, the significance of that task to the overall representation, how the GAI tool will process the client's information, and the extent to which knowledge of the lawyer's use of the GAI tool would affect the client's evaluation of or confidence in the lawyer's work.

Even when Rule 1.6 does not require informed consent and Rule 1.4 does not require a disclosure regarding the use of GAI, lawyers may tell clients how they employ GAI tools to assist in the delivery of legal services. Explaining this may serve the interest of effective client communication. The engagement agreement is a logical place to make such disclosures and to identify any client instructions on the use of GAI in the representation.[44]

D. Meritorious Claims and Contentions and Candor Toward the Tribunal

Lawyers using GAI in litigation have ethical responsibilities to the courts as well as to clients. Model Rules 3.1, 3.3, and 8.4(c) may be implicated by certain uses. Rule 3.1 states, in part, that "[a] lawyer shall not bring or defend a proceeding, or assert or controvert and issue therein, unless there is a basis in law or fact for doing so that is not frivolous." Rule 3.3 makes it clear that lawyers cannot knowingly make any false statement of law or fact to a tribunal or fail to correct a material false statement of law or fact previously made to a tribunal.[45] Rule 8.4(c) provides that a

---

lawyer must disclose the use of a temporary lawyer to a client where the temporary lawyer's use constitutes a "significant development" in the matter and listing relevant considerations); N.Y. State Bar Ass'n, Comm on Prof'l Ethics 715, at 7 (1999) (opining that "whether a law firm needs to disclose to the client and obtain client consent for the participation of a Contract lawyer depends upon whether client confidences will be disclosed to the lawyer, the degree of involvement of the lawyer in the matter, and the significance of the work done by the lawyer"); D.C. Bar Op. 284, at 4 (1988) (recommending client disclosure "whenever the proposed use of a temporary lawyer to perform work on the client's matter appears reasonably likely to be material to the representation or to affect the client's reasonable expectations"); Fla. State Bar Ass'n, Comm. on Prof'l Ethics Op. 88-12, 1988 WL 281590, at *2 (1988) (stating that disclosure of a temporary lawyer depends "on whether the client would likely consider the information material");.

[44] For a discussion of what client notice and informed consent under Rule 1.6 may require, see section B.

[45] MODEL RULES R. 3.3(a) reads: "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

lawyer shall not engage in "conduct involving dishonesty, fraud, deceit or misrepresentation." Even an unintentional misstatement to a court can involve a misrepresentation under Rule 8.4(c). Therefore, output from a GAI tool must be carefully reviewed to ensure that the assertions made to the court are not false.

Issues that have arisen to date with lawyers' use of GAI outputs include citations to nonexistent opinions, inaccurate analysis of authority, and use of misleading arguments.[46]

Some courts have responded by requiring lawyers to disclose their use of GAI.[47] As a matter of competence, as previously discussed, lawyers should review for accuracy all GAI outputs. In judicial proceedings, duties to the tribunal likewise require lawyers, before submitting materials to a court, to review these outputs, including analysis and citations to authority, and to correct errors, including misstatements of law and fact, a failure to include controlling legal authority, and misleading arguments.

E. Supervisory Responsibilities

Model Rules 5.1 and 5.3 address the ethical duties of lawyers charged with managerial and supervisory responsibilities and set forth those lawyers' responsibilities with regard to the firm, subordinate lawyers, and nonlawyers. Managerial lawyers must create effective measures to ensure that all lawyers in the firm conform to the rules of professional conduct,[48] and supervisory lawyers must supervise subordinate lawyers and nonlawyer assistants to ensure that subordinate lawyers and nonlawyer assistants conform to the rules.[49] These responsibilities have implications for the use of GAI tools by lawyers and nonlawyers.

Managerial lawyers must establish clear policies regarding the law firm's permissible use of GAI, and supervisory lawyers must make reasonable efforts to ensure that the firm's lawyers and nonlawyers comply with their professional obligations when using GAI tools.[50] Supervisory obligations also include ensuring that subordinate lawyers and nonlawyers are trained,[51] including in the ethical and practical use of the GAI tools relevant to their work as well as on risks associated with relevant GAI use.[52] Training could include the basics of GAI technology, the capabilities and limitations of the tools, ethical issues in use of GAI and best practices for secure data handling, privacy, and confidentiality.

---

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."

[46] *See* DC Bar Op. 388 (2024).

[47] Lawyers should consult with the applicable court's local rules to ensure that they comply with those rules with respect to AI use. As noted in footnote 4, no one opinion could address every ethics issue presented when a lawyer uses GAI. For example, depending on the facts, issues relating to Model Rule 3.4(c) could be presented.

[48] *See* MODEL RULES R. 1.0(c) for the definition of firm.

[49] ABA Formal Op. 08-451, *supra* note 15.

[50] MODEL RULES R. 5.1.

[51] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 467 (2014).

[52] *See generally*, MODEL RULES R. 1.1, cmt. [8]. One training suggestion is that all materials produced by GAI tools be marked as such when stored in any client or firm file so future users understand potential fallibility of the work.

Lawyers have additional supervisory obligations insofar as they rely on others outside the law firm to employ GAI tools in connection with the legal representation. Model Rule 5.3(b) imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make "reasonable efforts to ensure that" the nonlawyer's conduct conforms with the professional obligations of the lawyer. Earlier opinions recognize that when outsourcing legal and nonlegal services to third-party providers, lawyers must ensure, for example, that the third party will do the work capably and protect the confidentiality of information relating to the representation.[53] These opinions note the importance of: reference checks and vendor credentials; understanding vendor's security policies and protocols; familiarity with vendor's hiring practices; using confidentiality agreements; understanding the vendor's conflicts check system to screen for adversity among firm clients; and the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement. These concepts also apply to GAI providers and tools.

Earlier opinions regarding technological innovations and other innovations in legal practice are instructive when considering a lawyer's use of a GAI tool that requires the disclosure and storage of information relating to the representation.[54] In particular, opinions developed to address cloud computing and outsourcing of legal and nonlegal services suggest that lawyers should:

- ensure that the [GAI tool] is configured to preserve the confidentiality and security of information, that the obligation is enforceable, and that the lawyer will be notified in the event of a breach or service of process regarding production of client information;[55]
- investigate the [GAI tool's] reliability, security measures, and policies, including limitations on the [the tool's] liability;[56]
- determine whether the [GAI tool] retains information submitted by the lawyer before and after the discontinuation of services or asserts proprietary rights to the information;[57] and
- understand the risk that [GAI tool servers] are subject to their own failures and may be an attractive target of cyber-attacks.[58]

F. Fees

Model Rule 1.5, which governs lawyers' fees and expenses, applies to representations in which a lawyer charges the client for the use of GAI. Rule 1.5(a) requires a lawyer's fees and expenses to be reasonable and includes a non-exclusive list of criteria for evaluating whether a fee

[53] ABA Formal Op. 08-451, *supra* note 15; ABA Formal. Op. 477R, *supra* note 6.
[54] *See* ABA Formal Op. 08-451, *supra* note 15.
[55] Fla. Bar Advisory Op. 12-3 (2013).
[56] *Id.* citing Iowa State Bar Ass'n Comm. on Ethics & Practice Guidelines Op. 11-01 (2011) [hereinafter Iowa Ethics Opinion 11-01].
[57] Fla. Bar Advisory Op. 24-1, *supra* note 4; Fla. Bar Advisory Op. 12-3, *supra* note 55; Iowa Ethics Opinion 11-01, *supra* note 56.
[58] Fla. Bar Advisory Op. 12-3, *supra* note 55; *See generally* Melissa Heikkila, *Three Ways AI Chatbots are a Security Disaster*, MIT TECHNOLOGY REVIEW (Apr. 3, 2023), www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/.

or expense is reasonable.[59] Rule 1.5(b) requires a lawyer to communicate to a client the basis on which the lawyer will charge for fees and expenses unless the client is a regularly represented client and the terms are not changing. The required information must be communicated before or within a reasonable time of commencing the representation, preferably in writing. Therefore, before charging the client for the use of the GAI tools or services, the lawyer must explain the basis for the charge, preferably in writing.

GAI tools may provide lawyers with a faster and more efficient way to render legal services to their clients, but lawyers who bill clients an hourly rate for time spent on a matter must bill for their actual time. ABA Formal Ethics Opinion 93-379 explained, "the lawyer who has agreed to bill on the basis of hours expended does not fulfill her ethical duty if she bills the client for more time than she has actually expended on the client's behalf."[60] If a lawyer uses a GAI tool to draft a pleading and expends 15 minutes to input the relevant information into the GAI program, the lawyer may charge for the 15 minutes as well as for the time the lawyer expends to review the resulting draft for accuracy and completeness. As further explained in Opinion 93-379, "If a lawyer has agreed to charge the client on [an hourly] basis and it turns out that the lawyer is particularly efficient in accomplishing a given result, it nonetheless will not be permissible to charge the client for more hours than were actually expended on the matter,"[61] because "[t]he client should only be charged a reasonable fee for the legal services performed."[62] The "goal should be solely to compensate the lawyer fully for time reasonably expended, an approach that if followed will not take advantage of the client."[63]

The factors set forth in Rule 1.5(a) also apply when evaluating the reasonableness of charges for GAI tools when the lawyer and client agree on a flat or contingent fee.[64] For example, if using a GAI tool enables a lawyer to complete tasks much more quickly than without the tool, it may be unreasonable under Rule 1.5 for the lawyer to charge the same flat fee when using the GAI tool as when not using it. "A fee charged for which little or no work was performed is an unreasonable fee."[65]

The principles set forth in ABA Formal Opinion 93-379 also apply when a lawyer charges GAI work as an expense. Rule 1.5(a) requires that disbursements, out-of-pocket expenses, or additional charges be reasonable. Formal Opinion 93-379 explained that a lawyer may charge the

---

[59] The listed considerations are (1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly; (2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer; (3) the fee customarily charged in the locality for similar legal services; (4) the amount involved and the results obtained; (5) the time limitations imposed by the client or by the circumstances; (6) the nature and length of the professional relationship with the client; (7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and (8) whether the fee is fixed or contingent.

[60] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 93-379, at 6 (1993) [hereinafter ABA Formal Op. 93-379].

[61] *Id.*

[62] *Id.* at 5.

[63] *Id.*

[64] *See, e.g.*, *Williams Cos. v. Energy Transfer LP*, 2022 Del. Ch. LEXIS 207, 2022 WL 3650176 (Del. Ch. Aug. 25, 2022) (applying same principles to contingency fee).

[65] Att'y Grievance Comm'n v. Monfried, 794 A.2d 92, 103 (Md. 2002) (finding that a lawyer violated Rule 1.5 by charging a flat fee of $1,000 for which the lawyer did little or no work).

client for disbursements incurred in providing legal services to the client. For example, a lawyer typically may bill to the client the actual cost incurred in paying a court reporter to transcribe a deposition or the actual cost to travel to an out-of-town hearing.[66] Absent contrary disclosure to the client, the lawyer should not add a surcharge to the actual cost of such expenses and should pass along to the client any discounts the lawyer receives from a third-party provider.[67] At the same time, lawyers may not bill clients for general office overhead expenses including the routine costs of "maintaining a library, securing malpractice insurance, renting of office space, purchasing utilities, and the like."[68] Formal Opinion 93-379 noted, "[i]n the absence of disclosure to a client in advance of the engagement to the contrary," such overhead should be "subsumed within" the lawyer's charges for professional services.[69]

In applying the principles set out in ABA Formal Ethics Opinion 93-379 to a lawyer's use of a GAI tool, lawyers should analyze the characteristics and uses of each GAI tool, because the types, uses, and cost of GAI tools and services vary significantly. To the extent a particular tool or service functions similarly to equipping and maintaining a legal practice, a lawyer should consider its cost to be overhead and not charge the client for its cost absent a contrary disclosure to the client in advance. For example, when a lawyer uses a GAI tool embedded in or added to the lawyer's word processing software to check grammar in documents the lawyer drafts, the cost of the tool should be considered to be overhead. In contrast, when a lawyer uses a third-party provider's GAI service to review thousands of voluminous contracts for a particular client and the provider charges the lawyer for using the tool on a per-use basis, it would ordinarily be reasonable for the lawyer to bill the client as an expense for the actual out-of-pocket expense incurred for using that tool.

As acknowledged in ABA Formal Opinion 93-379, perhaps the most difficult issue is determining how to charge clients for providing in-house services that are not required to be included in general office overhead and for which the lawyer seeks reimbursement. The opinion concluded that lawyers may pass on reasonable charges for "photocopying, computer research, . . . and similar items" rather than absorbing these expenses as part of the lawyers' overhead as many lawyers would do.[70] For example, a lawyer may agree with the client in advance on the specific rate for photocopying, such as $0.15 per page. Absent an advance agreement, the lawyer "is obliged to charge the client no more than the direct cost associated with the service (i.e., the actual cost of making a copy on the photocopy machine) plus a reasonable allocation of overhead expenses directly associated with the provision of the service (e.g., the salary of the photocopy machine operator)."[71]

---

[66] ABA Formal Op. 93-379 at 7.
[67] *Id.* at 8.
[68] *Id.* at 7.
[69] *Id.*
[70] *Id.* at 8.
[71] *Id.* Opinion 93-379 also explained, "It is not appropriate for the Committee, in addressing ethical standards, to opine on the various accounting issues as to how one calculates direct cost and what may or may not be included in allocated overhead. These are questions which properly should be reserved for our colleagues in the accounting profession. Rather, it is the responsibility of the Committee to explain the principles it draws from the mandate of Model Rule 1.5's injunction that fees be reasonable. Any reasonable calculation of direct costs as well as any reasonable allocation of related overhead should pass ethical muster. On the other hand, in the absence of an agreement to the contrary, it is impermissible for a lawyer to create an additional source of profit for the law firm beyond that which is contained in the provision of professional services themselves. The lawyer's stock in trade is the sale of legal services, not photocopy paper, tuna fish sandwiches, computer time or messenger services." *Id.*

These same principles apply when a lawyer uses a proprietary, in-house GAI tool in rendering legal services to a client. A firm may have made a substantial investment in developing a GAI tool that is relatively unique and that enables the firm to perform certain work more quickly or effectively. The firm may agree in advance with the client about the specific rates to be charged for using a GAI tool, just as it would agree in advance on its legal fees. But not all in-house GAI tools are likely to be so special or costly to develop, and the firm may opt not to seek the client's agreement on expenses for using the technology. Absent an agreement, the firm may charge the client no more than the direct cost associated with the tool (if any) plus a reasonable allocation of expenses directly associated with providing the GAI tool, while providing appropriate disclosures to the client consistent with Formal Opinion 93-379. The lawyer must ensure that the amount charged is not duplicative of other charges to this or other clients.

Finally, on the issue of reasonable fees, in addition to the time lawyers spend using various GAI tools and services, lawyers also will expend time to gain knowledge about those tools and services. Rule 1.1 recognizes that "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment [8] explains that "[t]o maintain the requisite knowledge and skill [to be competent], a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engaging in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."[72] Lawyers must remember that they may not charge clients for time necessitated by their own inexperience.[73] Therefore, a lawyer may not charge a client to learn about how to use a GAI tool or service that the lawyer will regularly use for clients because lawyers must maintain competence in the tools they use, including but not limited to GAI technology. However, if a client explicitly requests that a specific GAI tool be used in furtherance of the matter and the lawyer is not knowledgeable in using that tool, it may be appropriate for the lawyer to bill the client to gain the knowledge to use the tool effectively. Before billing the client, the lawyer and the client should agree upon any new billing practices or billing terms relating to the GAI tool and, preferably, memorialize the new agreement.

III. Conclusion

Lawyers using GAI tools have a duty of competence, including maintaining relevant technological competence, which requires an understanding of the evolving nature of GAI. In

---

[72] MODEL RULES R. 1.1, cmt. [8] (emphasis added); *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 498 (2021).

[73] Heavener v. Meyers, 158 F. Supp. 2d 1278 (E.D. Okla. 2001) (five hundred hours for straightforward Fourth Amendment excessive-force claim and nineteen hours for research on Eleventh Amendment defense indicated excessive billing due to counsel's inexperience); *In re* Poseidon Pools of Am., Inc., 180 B.R. 718 (Bankr. E.D.N.Y. 1995) (denying compensation for various document revisions; "we note that given the numerous times throughout the Final Application that Applicant requests fees for revising various documents, Applicant fails to negate the obvious possibility that such a plethora of revisions was necessitated by a level of competency less than that reflected by the Applicant's billing rates"); Att'y Grievance Comm'n v. Manger, 913 A.2d 1 (Md. 2006) ("While it may be appropriate to charge a client for case-specific research or familiarization with a unique issue involved in a case, general education or background research should not be charged to the client."); *In re* Hellerud, 714 N.W.2d 38 (N.D. 2006) (reduction in hours, fee refund of $5,651.24, and reprimand for lawyer unfamiliar with North Dakota probate work who charged too many hours at too high a rate for simple administration of cash estate; "it is counterintuitive to charge a higher hourly rate for knowing less about North Dakota law").

using GAI tools, lawyers also have other relevant ethical duties, such as those relating to confidentiality, communication with a client, meritorious claims and contentions, candor toward the tribunal, supervisory responsibilities regarding others in the law office using the technology and those outside the law office providing GAI services, and charging reasonable fees. 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.

Appendix L

AI in Rare Disease Research

Patient Control, Global Law, Bias, and IP Ownership

The Stakes: Why Governance Matters

- Rare disease AI amplifies value AND risk
- Small datasets = highly linkable, cross-border flows
- Governance is a product feature, not a compliance afterthought

Ground rule for this session:

  - Black-letter law vs regulatory guidance vs best practice
  - Each will be marked clearly

SECTION 1: Patient Rights

How do we ensure patients with rare diseases retain control over their data and medical decisions when AI is involved?

What 'Control' Means Operationally [LAW]

Control over DECISIONS:

• GDPR Art. 22(1): Right not to be subject to decisions "based solely on automated processing" with legal/similarly significant effects

• Workflow-dependent: is the decision truly 'solely automated'?

Control over PROCESS:

• ICO guidance: Rights to challenge, seek human review

• DPIA required for high-risk automated decision-making

• Must prevent errors, bias, and discrimination

[LAW] = Black-letter law + regulatory guidance

DILEMMA: When Does AI Cross the Line?

SCENARIO

:An AI tool flags "low probability of eligibility" for a rare disease trial. The site never contacts the patient.

QUESTION:

Is this "solely automated decision-making"?

If not, what KIND of human involvement makes it real rather than rubber-stamping?

THINK ABOUT:

- Who reviews the output?
- What evidence do they consider?
- Can they override?
- Is it documented?

Practical Design Moves [BEST PRACTICE]

1. Build a "contestability" pathway:
   - Who receives challenges?
   - What evidence is reviewed?
   - What timeline?
   - Treat as part of product workflow, not a mailbox

2. Use DPIAs as a design artifact:
   - Not just a filing exercise
   - ICO treats solely automated decisions as high-risk
   - Document safeguards, human review, bias prevention

3. Transparency in consent materials:
   - Explain when/how AI is used
   - Clarify AI's role: support vs decision-maker

SECTION 2: Data Ownership, Consent & Secondary Use

Who owns the data collected?

How do we handle informed consent for AI algorithms that continue learning and evolving?

Stop Asking "Who Owns the Data?" [GUIDANCE]

Better question: Who is controller/processor, and what rights/duties attach?

Controller/Processor Framework:

• Controller: decides purposes and means of processing

• Processor: processes on behalf of controller

• Joint controllers: jointly determine purposes/means

Data subject rights under GDPR/UK GDPR:

• Access, rectification, erasure (where applicable)

• Restriction, portability, objection

This framework scales across jurisdictions

HIPAA has parallel concepts (covered entity/business associate)

Evolving Models: The Consent Challenge [GUIDANCE]

Problem: Purpose limitation vs continuous improvement

DILEMMA: If a patient withdraws, can you realistically remove their influence from a trained model?

Operational Requirements:

• Versioning + change-impact process for:

- Training data additions

- Model updates

- Downstream use changes

• Set expectations transparently:

- Disclose technical limits of withdrawal

- Document what "erasure" means in practice

• Broad consent + governance:

- EU/UK accept broad consent for defined field

- Plus oversight, ethics approval, opt-out rights

SECTION 3: Global Privacy Regulations

How international data protection laws impact AI collaboration in rare disease research, trials, and treatment

HIPAA, GDPR, UK GDPR, and beyond

What You Can State with Confidence [LAW]

GDPR/UK GDPR Article 22:

- Restricts solely automated decisions with legal/similarly significant effects
- ICO: High risk requires DPIA and safeguards
- Must prevent errors, bias, discrimination

UK-US Data Bridge:

- UK organisations can transfer to US organisations certified to UK Extension to EU-US Data Privacy Framework
- Without needing additional safeguards (for certified recipients)
- KEY: Check certification status in procurement

HIPAA (US):

- Covered entities + business associates
- De-identification: Safe Harbor or Expert Determination

Cross-Border Collaboration 'Tripwires' [GUIDANCE]

Tripwire 1: Assuming bridge applies to any US vendor

- UK-US Data Bridge only applies to certified US organisations
- Action: Check certification status in procurement
- Fallback: Use SCCs + transfer impact assessment

Tripwire 2: "Compliant in one jurisdiction = compliant everywhere"

- Rare disease programs are multi-actor, multi-jurisdiction
- Need: Single documented data flow map
- Shows: What data, from where, to whom, under what law

Tripwire 3: Over-relying on de-identification in rare disease

- Small-N datasets = higher re-identification risk
- Need: Privacy risk assessment, not just checkbox

DILEMMA: Data to Models or Models to Data?

SCENARIO:

Your best rare disease dataset is in UK/EU.

Your best AI model team is in the US.

QUESTION:

Do you move data to models—or models to data?

CONSIDERATIONS:

• Is the US recipient certified to Data Bridge/DPF?

• Can you use federated learning instead?

• Can you train on synthetic/de-identified data?

• What does your DPIA say about transfer risks?

No universal right answer—governance and risk tolerance matter

SECTION 4: Algorithmic Bias and Fairness

Addressing inequities in datasets that can lead to misdiagnosis or lack of recognition of symptoms in underrepresented populations

Why rare disease is a worst-case test for bias

Bias Pathways in Medical AI [EVIDENCE]

Sources of bias:

• Underrepresentation in training data

- Models tuned on majority populations generalize poorly

- Genetic/imaging data from European-ancestry patients

• Structural and labeling bias

- Historical underdiagnosis of certain groups

- Ground truth labels carry past inequities

Rare disease amplification:

• Small datasets magnify representation gaps

• Can entrench diagnostic delay for underrepresented groups

• Trial matching tools may never surface some subgroups

ICO guidance: Automated decision-making must prevent bias/discrimination

Mitigation + The Fairness Dilemma [BEST PRACTICE]

Governance and technical measures:

• Dataset documentation: demographics, gaps, known biases

• Subgroup performance evaluation (where feasible)

• Federated learning to bring in diverse sites

• Post-deployment monitoring and recalibration

DILEMMA:

If improving fairness reduces overall accuracy, what do you optimize:

• Average performance?

• Worst-group harm?

You need an articulated ethical position—one that can be defended to regulators, ethics committees, and patients

SECTION 5: Intellectual Property

Who owns AI-generated insights?

Researchers, institutions, or patients?

Navigating patents and proprietary algorithms

AI Inventorship and Ownership [LAW]

USPTO Guidance (US):

• Only natural persons can be inventors

• Inventorship = significant contribution to each claim (Pannu factors)

• AI assistance doesn't make AI an inventor

• Document human contributions contemporaneously

Practical implications for rare disease AI:

• If AI suggests genotype-phenotype correlation or biomarker:

- Humans who design, run, interpret can be inventors

- Problem formulation, selection, interpretation matter

• Contracts must define IP allocation:

- Data contributors vs model developers

- Institutions vs sponsors vs vendors

DILEMMA: If value came from patients' data but patent came from your model, what is fair "return"?

• Access commitments? Pricing? Reinvestment?

Three Questions to Take Away

1. Where in our workflow could an AI output become a "solely automated" decision in practice?

- Who reviews? Can they override? Is it documented?

2. Which of our US vendors are actually eligible under the UK Extension/DPF—and what is our fallback transfer mechanism when they aren't?

- Check certification status in procurement

3. What harm are we willing to tolerate if subgroup performance differs—and who signs that decision?

- Average performance vs worst-group harm
- Articulated ethical position for regulators, ethics committees, patients

why should I believe what you tell me about AI and healthcare laws

That's a very fair question. You *shouldn't* believe me blindly — especially about something as important as AI and healthcare laws.

Here's how to think about it rationally:

1️⃣ I'm not an authority — I'm a tool

I'm not a regulator, lawyer, or policymaker. I generate responses based on patterns in the data I was trained on. When discussing healthcare law, I'm summarizing publicly available information such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- 21st Century Cures Act
- General Data Protection Regulation (GDPR)
- U.S. Food and Drug Administration (FDA) guidance on AI/ML medical devices

But I am not the source of truth — those institutions are.

2️⃣ You should verify high-stakes information

Healthcare law is:

- Jurisdiction-specific
- Frequently updated
- High-risk if wrong

For anything involving compliance, patient data, liability, reimbursement, or regulatory approval, you should:

- Check official government websites
- Consult a qualified healthcare attorney
- Review primary source legislation

- Verify the publication date of guidance

If you ever want, I can help you:

- Find the exact statutory language
- Compare multiple regulatory frameworks
- Identify what is settled vs. evolving

3️⃣ My strengths (and limits)

Where I'm strong:

- Explaining complex frameworks clearly
- Comparing international approaches
- Breaking down regulatory categories
- Translating legal language into plain English

Where you should be cautious:

- Very recent regulatory changes
- State-specific rules
- Active litigation
- Strategic legal decisions

4️⃣ Healthy skepticism is smart

With AI in healthcare — whether it's FDA approval pathways, HIPAA compliance, algorithmic bias, or reimbursement policy — blind trust is dangerous. That applies to:

- AI tools
- Blogs
- News articles
- Even consultants

Trust should come from:

- Transparency
- Source citations
- Cross-verification
- Expertise accountability

If you'd like, tell me what specifically concerns you about AI and healthcare laws — accuracy, bias, liability, regulatory capture, data privacy?

I can walk through it carefully and show you exactly where the information comes from and how confident we should be about it.

Why didn't you mention the AI Act in your prior answer?

Good catch — that's a reasonable challenge.

I didn't mention the Artificial Intelligence Act in my previous answer because I was giving examples of **well-established healthcare-specific laws and regulators** (HIPAA, GDPR, FDA oversight) rather than broader AI regulation frameworks.

But you're right: if we're talking about AI *and* healthcare law in 2026, the AI Act absolutely belongs in that conversation.

Here's why it didn't automatically come up:

1️⃣ Scope difference

- **HIPAA** → healthcare data privacy (U.S.)
- **GDPR** → personal data protection (EU)
- **FDA guidance** → medical device regulation (U.S.)
- **AI Act** → horizontal AI regulation across all sectors in the EU

The AI Act is not healthcare-specific — it regulates AI systems based on **risk categories**, including high-risk systems used in medical devices.

2️⃣ The AI Act intersects with healthcare through risk classification

Under the AI Act:

- AI systems used as medical devices are typically classified as **"high-risk"**

- That triggers strict obligations (risk management, documentation, transparency, human oversight)

But actual market approval for medical AI in Europe still runs through:

- The **Medical Device Regulation (MDR)**
- Notified bodies
- CE marking processes

So healthcare AI in the EU sits at the intersection of:

- AI Act
- MDR
- GDPR

3️⃣ Why your question matters

If someone talks about "AI regulation in healthcare" in Europe and doesn't mention the AI Act, that's now incomplete.

Your question highlights something important:
A trustworthy explanation should include *both* domain-specific law (healthcare) and cross-sector AI regulation.

If you'd like, we can dig into something specific:

- How the AI Act changes compliance for AI medical startups?
- Whether it conflicts with MDR?
- How enforcement will actually work?
- Whether it meaningfully protects patients?

That's where things get interesting — and more nuanced.