SpencerFane®

If You or Your Clients Are Using AI, Here is What You Should Know

The laws and regulations around data privacy and cybersecurity are ever-changing, and with the rapidly growing popularity of artificial intelligence (AI), we are starting to see more regulatory action at the federal and individual state levels specific to AI. Lawmakers on both levels are driven by the desire to provide protections for consumers and intellectual property rights. With five states recently implementing regulations around the use of AI, and more likely on the horizon, it is important to know what your business can do to avoid violating the law.

Where is the Law Regulating AI Today

Like with data privacy, there is no comprehensive law in the U.S. at the federal level governing the use of AI. While there had been an executive order in place to fund research into AI and how to use it safely and regulate it properly, that was rescinded early in 2025. Currently there are a handful of executive orders in place, and they revolve around three main objectives of the White House: accelerating AI innovation; building American AI infrastructure; and leading in international AI diplomacy and security. The following are the current federal and state rules and regulations in effect or coming soon.

Current Federal AI Regulations:

- The Take It Down Act criminalizes the non-consensual posting of intimate images, including deepfakes. It is enforced by the FTC and requires platforms to remove such content within 48 hours of notification from a victim.
- Executive Order Promoting the Export of the American AI Technology Stack tasks the Secretary of Commerce with establishing and implementing an AI export

program by October 21, 2025. The directive is for a program to the creation and launching of U.S. full-stack AI export packages. “Full stack development” is the construction of both front- and back-end applications, and the use of AI can make this process much more efficient.
- There is also an Executive Order in place to promote and provide funding for data centers across the U.S. The Accelerating Federal Permitting of Data Center Infrastructure Executive Order provides the Secretary of Commerce with the ability to fund data center projects, including the infrastructure needed to power those data centers as they consume high amounts of energy and water.

New State AI Laws

The following states have passed laws specifically regulating the use of AI. Most of the laws require notifying consumers when AI is being used, and restrictions around using it to make decisions where bias (even if unintentional) could influence a result. Each of these have differences in who must comply, so you should reference the specific statues, but a high-level summary of each is below.

- The Utah Artificial Intelligence Policy Act was amended in May 2025. It requires that when a consumer is interacting with an AI system in certain situations, the consumer must receive notice in the beginning and throughout the use that they are interacting with AI and not a human. Notice is required where there is sensitive data involved, such as biometric, health, and financial data, as well as where AI is used to provide recommendation, information, or advice around certain decisions, such as approval for a loan or medical and mental health advice.
- Maine enacted the Chatbot Disclosure Act, which requires that consumers be notified when they are not engaging with a human where a reasonable consumer may not know they are engaging with AI (e.g., customer service online chats). The Act prohibits the use of AI chatbots or similar technologies in a manner that could mislead or deceive the consumer into thinking they are engaging with a real human. Notice of the use of an AI chatbot must be clear and conspicuous.
- In June 2025, the Texas Responsible Artificial Intelligence Governance Act was signed into law, and it goes into effect January 1, 2026. The law applies to

government entities and anyone (a business or individuals) that promotes, advertises, or conducts business in Texas, produces a product or service that Texas residents use, or develops or deploys an AI system in Texas. Government agencies are specifically prohibited from using AI for certain purposes, such as assigning a social score or using biometric data without the consumer's consent. Other entities are prohibited from using AI to incite or encourage violence, infringe or restrict another's rights under the U.S. Constitution, discriminate, or produce or distribute explicit content (including deepfakes). This law also impacts the developers and deployers of these AI systems.

- Arkansas recently enacted a law to protect and clarify who owns AI generated content. The new law states that the person who supplied the information to train a model owns the end model, unless there is a contract that says otherwise, or the information was supplied by an employee at the employer's instruction (then it is owned by the employer as work product). Similarly, where a person inputs information into a generative AI tool, the content that is generated is owned by that person, so long as it does not infringe on the existing intellectual property rights of another.
- The Colorado Artificial Intelligence Act will go into effect February 1, 2026, and is one of the most comprehensive AI laws in the U.S. to date, covering a variety of issues, and may require an update to existing privacy notices. With exceptions for small businesses and certain sectors that are already highly regulated, it generally applies to anyone using an AI system that interacts with Colorado residents. Use of AI must be disclosed to the consumer (Colorado residents) when they are interacting with AI, unless it is "obvious." AI must be regulated where it is considered a "high risk" AI system. It is considered high risk where it is used for making decisions or is a substantial factor in the decision-making process in certain areas, such as education, employment, financial/lending, government services, health care, housing, insurance, and legal. The developers of these systems are required to provide substantial documentation on the development process, including how the system was developed and evaluated to mitigate discrimination. The users of high-risk AI systems (e.g., a company using an AI system to evaluate job applicants) must use reasonable care, implement a risk management policy and program, and complete an impact assessment. Use of AI must also be disclosed in deployer's privacy policy/notice, before a decision using the AI is made, and developers and deployers must notify

Colorado Attorney General of its use.

Considerations If You Use AI

First and foremost, you should evaluate how you use AI, and if you use generative AI, what you do with the information generated. You should also consider who (residents of which states and countries) may be interacting with AI on your platform, and which laws may apply to you. You may want to consider updating your privacy policy / notice to address AI use. Having a thorough understanding of what information you have, where it comes from, where it is stored, and how you use it is extremely important for general data privacy and security, and with the ever-changing landscape in the area and the use of AI, it will be even more imperative moving forward.

If you own or manage a business and have employees, you should have a policy around the use of AI. It is very likely that your employees are using AI in some manner, so to protect your business you should dictate how your employees use it for work. Consider if you will allow use of a company provided device with AI, or if they must disclose to you if part of their work was developed using AI.

With the focus in some states around restrictions and controls on developers of AI systems, and deployers (those entities that use the AI systems), consider how this impacts your contract negotiations with certain service providers. For example, if you or your business will use an AI system to sort through job applications for potential applicants you would like to interview, and you are subject to the CO AI Act, you are now the deployer of a high-risk AI system. In the contract with the developer of the high-risk AI system, you should include clauses that pass through certain compliance matters to the developer and ensure that they are compliant with the applicable laws. Likewise, if you or your company is the developer of certain AI systems, consider the contracts you have with your customers, and make it clear what you do and do not do for them, such as if you will provide the required notices or if that falls on the deployer.

In addition to concerns about bias, AI has also provided “hallucinations,” which are made up facts to provide the requested results. This has happened in the legal filed multiple times, with AI making up fake case law and citations. Attorneys are being

reprimanded for these mistakes, and anyone that uses AI for drafting purposes should take caution. AI is only as good as the information it was provided to "learn," and garbage going in leads to garbage coming out. AI can be a great resource, but users still need to fact check and cite check the output – your reputation could be at risk if you do not.

If you or your company uses AI, the best practice is to engage with a professional who knows the law early on and can help you manage and mitigate risk.

This blog was drafted by Jessica Brigman, an attorney in the Spencer Fane St. Cloud, Minnesota, office. For more information, visit www.spencerfane.com.

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.