
Wisconsin Legislative Council

STAFF BRIEF



STUDY COMMITTEE ON THE REGULATION OF ARTIFICIAL INTELLIGENCE IN WISCONSIN

Brian Larson, Principal Attorney
Tom Koss and Patrick Ward, Staff Attorneys

July 17, 2024

SB-2024-02

The Wisconsin Legislative Council is a nonpartisan legislative service agency. Among other services provided to the Wisconsin Legislature, staff of the Wisconsin Legislative Council conduct study committees under the direction of the Joint Legislative Council.

Established in 1947, the Joint Legislative Council directs study committees to study and recommend legislation regarding major policy questions facing the state. Study committee members are selected by the Joint Legislative Council and include both legislators and citizen members who are knowledgeable about a study committee's topic.

This staff brief was prepared by the Wisconsin Legislative Council staff as an introduction for study committee members to the study committee's topic.

INTRODUCTION

Artificial intelligence (AI) is a technology that has the potential to affect every aspect of modern life. Recent advances in AI, including increased access, have generated significant interest from regulators, business leaders, and the public. While many of its potential uses are still conjecture, AI is already used in numerous ways in fields such as health care, and in the generation of text and images. Recognizing the interest in these benefits and risks, many states have enacted legislation regulating the use of AI.

In response to legislative interest in the effect of AI, the Joint Legislative Council (JLC) created the Study Committee on the Regulation of AI in Wisconsin and directed it to review current uses of AI technology and make recommendations for legislation regarding the use and development of AI technology. The JLC specified that the study committee may review the use of AI in disinformation and artificial imagery and the feasibility of establishing a process to ensure continued state monitoring of high-risk use of AI.

Consistent with the JLC's particular focus on the potential harms associated with the use and misuse of AI, this staff brief provides information on the following topics to assist the committee members in carrying out the committee's charge:

- **Part I** provides an overview of AI, how it can be defined for the purposes of state regulations, and its current and potential uses.
- **Part II** describes recent developments related to AI in Wisconsin and relevant state laws.
- **Part III** provides an overview of legislation enacted regulating the use of AI by the federal government, other states, and the European Union.

PART I | OVERVIEW OF AI

WHAT IS AI?

While the concept of AI dates back to the 1950s, recent technological advances have led to an increased use of, and interest in, AI. The term “artificial intelligence” has been conceptualized in various ways throughout the history of AI, but generally refers to computerized systems that work and react in ways that are commonly thought to require intelligence, such as the ability to learn, solve problems, perform complex tasks, and achieve goals under varying conditions.¹

There is not yet consensus on how AI should be defined for purposes of regulation. The Organization for Economic Cooperation and Development (OECD) and its member countries, which includes the United States, have pursued a consensus definition of AI to act as the foundation for AI regulations.² The European Union adopted a definition similar to the OECD definition, as have some states. Currently, the OECD defines an AI system as follows:

[A] machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

[[OECD](#), *AI Principles overview* (accessed July 17, 2024).]

As shown in Part III, states that have enacted legislation regulating AI have taken different approaches. Examples of various definitions of AI in state law include the following:

- Indiana defines AI as computing technology that is capable of simulating human learning, reasoning, and deduction through certain processes, such as identifying patterns in data. [IC s. 4-13 1-5.]
- New Mexico defines AI as a machine-based or computer-based system that through hardware or software uses input data to emulate the structure and characteristics of input data in order to generate synthetic content, including images, video, or audio. [s. 1-19-26 C. NMSA 1978.]
- Texas defines AI systems as systems that are capable of both of the following: (1) perceiving an environment through data acquisition and processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given a specific goal; and (2) learning and adapting behavior by analyzing how the environment is affected by prior actions. [s. 2054.621 (2), Texas Government Code.]

¹ Congressional Research Service, *Artificial Intelligence: Overview, Recent Advances, and Considerations for the 118th Congress*, [CRS Report](#) (August 4, 2023).

² The OECD is a member organization comprised of 38 member countries, including Australia, Canada, Mexico, the United Kingdom, the United States, and many countries in the European Union and works with policy makers, stakeholders and citizens to establish evidence-based international standards and to find solutions to social, economic, and environmental challenges. [<https://www.oecd.org/en/about.html>.]

OTHER CONCEPTS RELATING TO AI

While a full discussion of how AI systems are created is beyond the scope of this staff brief, certain common concepts related to AI are discussed below.

First, **generative AI** is one type of AI. Generative AI can generate new content, such as text, images, and videos, by learning patterns from pre-existing data. Generative AI can create new content based on different inputs, which are also referred to as “prompts.”³ Examples of generative AI include: chatbots, which can generate text from prompts based on training data, and applications that can generate images from prompts.

Large language models (LLMs) are a subset of generative AI and are used to build many AI applications. LLMs can recognize, predict, translate, summarize, and generate language. They must be trained on large amounts of data. Most of this data is obtained, or “scraped,” from publicly available web pages.⁴

Machine learning is considered a subset of AI. Machine learning has been defined as “the field of study that gives computers the ability to learn without being explicitly programmed.” It is used for applications such as chatbots, predictive text, medical imaging and diagnostics, and recommendation algorithms.⁵

There are three subcategories of machine learning: (1) supervised machine learning models, which are trained with labeled data sets that allow the models to learn and become increasingly accurate; (2) unsupervised machine learning models, which look for patterns and trends in unlabeled data; and (3) reinforcement machine learning models, which train machines through trial and error to take the best action by establishing a reward system.⁶

Machine learning is associated with several other concepts. These concepts include **natural language processing**, which is a field of machine learning where machines learn to recognize, understand, and respond to natural language and to create new text and translate between languages. Natural language processing enables technology like chatbots. A **neural network** is a type of machine learning network that is modeled on the human brain in which processing nodes are interconnected and organized into layers, where cells in each layer process input and produce an output that is sent to other neurons. A **deep learning network** is a neural network with many layers that can process extensive amounts of data by using different layers to accomplish different tasks.⁷ **Computer vision** uses machine learning and neural networks to obtain useful information from digital images, videos, and other visual inputs and to make recommendations or act when indicated.⁸

POTENTIAL USES OF AI

AI is poised to create many significant societal benefits. However, AI may also bring negative consequences, including by enabling offensive conduct or creating unintended effects.

Uses of AI can be found in various areas of society. For example, in business, an increasing number of companies have incorporated AI into their operations for marketing automation,

³ Congressional Research Service, *Generative Artificial Intelligence and Data Privacy: A Primer*, [CRS In Focus](#) (May 23, 2023).

⁴ Id.

⁵ Sara Brown, *Machine Learning, Explained*, [MIT Management Sloan School](#), April 21, 2021.

⁶ Id.

⁷ Id.

⁸ IBM, [What is computer vision?](#) (accessed July 8, 2024).

virtual agents and chatbots, natural language processing, and data and text analytics. According to the U.S. Census Bureau, approximately 5 percent of firms used AI in February 2024, and about 6.6 percent are expected to use AI in fall of 2024.⁹

In health care, generative AI can improve communication between providers and patients; medical devices with machine learning can help with tasks like reading mammograms, diagnosing eye disease, and detecting heart problems; and chatbots can help alleviate loneliness experienced by seniors. In policing, machine learning allows law enforcement agencies to use facial recognition software to help identify people suspected of committing a crime. In transportation, autonomous vehicles use AI to analyze information that is continuously accumulated through cameras and sensors.¹⁰

More generally, experts have theorized that AI's capacity to accelerate scientific research could result in cures for disease and solutions for climate change and resource shortages, and that AI could dramatically increase the production of goods and services.¹¹

How AI will be used in the future is unknown, but some potential risks have been identified:

- *Surveillance and persuasion.* AI may be used to perform mass surveillance, detect activities, and exert targeted influence on individuals of interest.
- *Biased decision-making.* Use of AI in contexts such as the evaluation of parole and loan applications, or various other business processes, can result in decisions that are biased based on protected categories like race or gender.
- *Impacts on employment.* Increased use of AI may result in job displacement or job loss.
- *Safety-critical applications.* The use of AI for purposes such as driving cars and managing the water supplies of cities has led to fatal accidents.
- *Cybersecurity threats.* AI may contribute to the potency, survivability, and proliferation capability of malware.
- *Lethal autonomous weapons.* AI may be used to develop weapons that are scalable and can locate, select, and eliminate human targets without human intervention.¹²

Other sources of concern include the transparency and ethics of using AI in areas like research and education and the use of AI technology to create “deepfake” images or audio for political disinformation, fraud, harassment, or sexual exploitation.¹³

As described in Part III, some states have already enacted legislation related to some of these negative consequences. For example, as described in more detail in Part II, Wisconsin recently enacted legislation that requires disclosures in political communications created with the use of generative AI.

⁹ U.S. Census Bureau Center for Economic Studies, *Tracking Firm Use of AI in Real Time: A Snapshot from the Business Trends and Outlook Survey*, March 2024: [3.9](#).

¹⁰ Carla K. Johnson, *Is your doctor using AI?*, [Associated Press](#), March 13, 2024; Terry Spencer, *Chatty robot helps seniors fight homelessness through AI companionship*, [Associated Press](#), December 22, 2023; and Darrell M. West and John R. Allen, *How artificial intelligence is transforming the world*, [Brookings](#), April 24, 2018.

¹¹ Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed. 2020) at 31–32.

¹² *Id.*

¹³ Congressional Research Service, *Generative Artificial Intelligence and Data Privacy: A Primer*, [CRS In Focus](#) (May 23, 2023), and David Klepper, *A congressman wanted to understand AI. So he went back to a college classroom to learn*, [Associated Press](#), April 11, 2024.

PART II | DEVELOPMENTS RELATED TO AI IN WISCONSIN

In the 2023-24 legislative session, the Legislature enacted two laws related to AI: one that requires disclosure of the use of generative AI in political advertisements, and one to prohibit the possession of virtual child pornography. Several other bills related to AI were also introduced, and both the Governor and Assembly Speaker convened task forces related to AI.

LEGISLATION ENACTED RELATED TO AI

2023 Wisconsin Act 123

2023 Wisconsin Act 123 requires disclosure of certain types of political advertisements that incorporate audio or video content that is substantially produced in whole or in part by means of generative AI.

Wisconsin has enacted two provisions related to AI, both in the 2023-24 session.

Under Act 123, any audio or video communication that contains express advocacy, contains issue advocacy, or supports or opposes a referendum must include a disclosure if the communication contains “synthetic media,” which is defined as audio or video content that is substantially produced in whole or in part by means of generative AI.¹⁴

The act requires the Wisconsin Ethics Commission to investigate violations of this requirement in the same manner as it currently does for similar violations of disclosure requirements over which it has regulatory authority; violations are subject to a forfeiture of up to \$1,000 per violation. Under the act, the Ethics Commission may promulgate rules to create limited exceptions to the act’s disclosure requirements.

2023 Wisconsin Act 224

2023 Wisconsin Act 224 created a new crime titled, *Possession of virtual child pornography*, that prohibits certain acts relating to obscene material¹⁵ that contains a “depiction of a purported child,” defined as a visual representation that appears to depict an actual child, but may or may not depict an actual child.

Specifically, the new crime prohibits receiving, distributing, producing, or possessing, or accessing in any way with the intent to view, obscene material that contains a depiction of a purported child engaging in sexually explicit conduct, if the person: (1) knows that he or she received, distributed, produced, possessed, or accessed the material; and (2) knows, or reasonably should know, that the material contains a depiction of a purported child engaging in sexually explicit conduct.

Under the act, violations of the new crime are punishable as a Class D felony or, if the actor is under 18 years of age when the offense occurs, a Class I felony. The act imposes consequences

¹⁴ Act 123 exempts a broadcaster or other host or carrier of a political communication from liability for violations of the disclosure requirement and establishes that its provisions do not affect the rights of a broadcaster or other host or carrier under a federal law intended to protect the rights of a content host to monitor or limit the content it hosts.

¹⁵ The act defines “obscene material” as a photograph, film, motion picture, or digital or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, that: (a) the average person, applying contemporary community standards, would find appeals to the prurient interest if taken as a whole; (b) under contemporary community standards, describes or shows sexually explicit conduct in a patently offensive way; and (c) lacks serious literary, artistic, political, educational, or scientific value, if taken as a whole.

for violations of the new crime that are similar to those that apply when an individual is convicted of possession of child pornography. Those consequences include a mandatory three-year minimum period of confinement in prison as part of the individual's sentence, a requirement that the individual register as a sex offender with the Department of Corrections, and payment of a child pornography surcharge of \$500 for each image or copy of an image associated with the crime.

OTHER PROPOSALS RELATED TO AI

2023 Assembly Speaker's Task Force on AI

In 2023, Assembly Speaker Robin Vos established the Speaker's Task Force on AI to study the transformative potential of AI and make policy recommendations that ensure its responsible and ethical deployment. Specifically, the task force was asked to consider the use of AI tools by the public and private sectors, including automated decision tools, facial recognition, and generative AI.

The task force held four public hearings to receive testimony from invited speakers and the public. Some members of the task force and other members of the Legislature authored bills related to the subject of the hearings. The chairperson and vice-chairperson, on behalf of the task force, released a report describing the work of the task force and endorsing the legislation that had been authored, including the bills that became Act 123 and Act 224. The task force also recommended passage of Assembly Bill 1068, which is discussed below.¹⁶

2023 Assembly Bill 608 and 2023 Senate Bill 553

Current law generally prohibits capturing or distributing a representation depicting an intimate representation of a person under circumstances in which the person had a reasonable expectation of privacy and did not consent. [s. 942.09 (2), Stats.]

Companion bills 2023 Assembly Bill 608 and 2023 Senate Bill 553, relating to representations depicting nudity and providing a penalty, expanded this prohibition to apply not just to intimate representations but also to "synthetic intimate representations." This term is defined to mean a technologically generated representation that uses an identifiable person's face, likeness, or other distinguishing characteristic to depict an intimate representation of that person, regardless of whether the representation includes components that are artificial, legally generated, or generally accessible. Specifically, the bill prohibited posting, publishing, distributing, or exhibiting a synthetic intimate representation of an identifiable person with intent to coerce, harass, or intimidate that person.¹⁷

Neither bill was enacted. The Senate bill passed the Senate but was not acted upon by the Assembly.

2023 Assembly Bill 1068 and 2023 Senate Bill 1010

Companion bills 2023 Assembly Bill 1068 and 2023 Senate Bill 1010, relating to the use of AI by state agencies and staff reduction goals, did the following: (1) directed an audit of state agencies;

¹⁶ The task force also recommended Assembly Bill 466, relating to consumer data protection and providing a penalty, and LRB-5745/1, relating to artificially generated representations depicting nudity and providing a penalty, which was not introduced.

¹⁷ The bill also prohibited reproducing a sexually explicit representation of a person without consent.

(2) created agency reporting requirements; and (3) established goals for agencies to reduce their workforce needs through AI tools.

First, the bill directed the Legislative Audit Bureau to conduct an audit of how each state agency is using AI tools to increase efficiency in carrying out agency functions. The audit report would include at least the following:

- An inventory of the AI tools each agency is using, developing, or decommissioning, and the reason for the use, development, or decommission of each tool, including any initiatives regarding the use of AI tools that an agency is undertaking.
- A summary of written guidelines governing the use of AI tools by employees and contractors of each agency.
- A summary of the policies and practices in place at each agency to ensure the privacy of personally identifiable information that the agency collects or uses with AI tools.
- A summary of the policies and practices of each agency to evaluate the data collected and used with AI tools, and the performance, effectiveness, and results of the AI tools.

Second, the bill required each state agency to submit a biennial report regarding its use of AI tools, including the following: (1) updates to the data found in the audit described above; (2) an explanation of the progress the agency is making towards any recommendations resulting from the audit; (3) an identification of full-time equivalent (FTE) positions within the agency whose work could be made more efficient with the use of AI tools; and (4) a description of the agency's progress towards reducing its FTE position needs relative to the positions authorized for the agency.

Finally, the bill established two requirements generally relating to the state's biennial budget process. First, it directed DOA to prepare a report, for delivery to the Joint Committee on Finance, summarizing the agency reports described above. Second, the bill directed each state agency's biennial budget request to include a proposal to reduce the agency's position authorizations for each year of the succeeding fiscal biennium relative to the agency's position authorizations for the 2023-24 fiscal year.

Neither bill was enacted. The Assembly bill passed the Assembly but was not acted upon by the Senate.

2023 Assembly Bill 1158 and 2023 Senate Bill 1072

Companion bills 2023 Senate Bill 1072 and 2023 Assembly Bill 1158, relating to a disclaimer required when interacting with generative AI that simulates conversation, prohibited any person from hosting or using on the person's digital platform, product, service, application, or web page generative AI that simulates what a human user would reasonably expect to be a conversation with, or instant message from, a human being, unless first providing the user a prominent and legible disclaimer that the generative AI is not a human being.

Neither bill was acted upon.

Governor's Task Force on Workforce and AI

In August 2023, Governor Tony Evers created the Governor's Task Force on Workforce and AI. He instructed the task force to gather and analyze information and produce an advisory action plan that includes certain information, such as an identification of the current state of generative AI's impact on Wisconsin's labor market and solutions to potential impacts on Wisconsin's key industries, occupations, and foundational skillsets. [[Executive Order #211.](#)]

For more information on the Governor’s task force, see the Department of Workforce Development [webpage](#).

OTHER RELEVANT STATE LAWS

Several current statutes do not apply directly to AI but may have implications for the use of AI. These laws are summarized below.

Defamation

The criminal prohibition and civil cause of action for defamation could be used to address instances of AI disinformation.

Under current law, any person who, with intent to defame, communicates any defamatory matter to a third person without the consent of the person defamed is guilty of a Class A misdemeanor. Defamatory matter is anything that exposes the other person to hatred, contempt, ridicule, degradation, or disgrace in society or injury in the other’s business or occupation. This prohibition, however, does not apply if the defamatory matter was true and was communicated with good motives and for justifiable ends. [s. [942.01](#), Stats.]

Wisconsin also provides a common law civil cause of action for defamation. The elements for such an action are the following: (1) a false statement; (2) the statement is communicated by speech, conduct, or writing to a person other than the person defamed; and (3) the communication is unprivileged and tends to harm one’s reputation as to lower him or her in the estimation of the community or to deter third persons from associating with or dealing with him or her. [*Torgerson v. Journal/Sentinel Inc.*, 210 Wis. 2d 524, 534 (1997); [Wis. JI-Civil 2500](#) (2022).] A person who has been defamed may recover compensatory and punitive damages.

Giving False Information for Publication

Similarly, state law prohibits communicating to a newspaper, magazine, or other publication any false statement concerning any person or any false and unauthorized advertisement, with intent that it be published and injure any person, if the person has knowledge that it is false. [s. [942.03](#), Stats.]

Representations Depicting Nudity

Wisconsin law prohibits certain actions related to the capture and distribution of representations depicting nudity, though it does not specifically address the creation or distribution of “deepfakes.” Specifically, current law prohibits the following, with certain exceptions:

- Capturing an intimate representation (generally, a representation depicting nudity or sexual conduct) without the consent of the person depicted under circumstances in which he or she has a reasonable expectation of privacy, if the person knows or has reason to know that the person depicted does not consent to the capture of the intimate representation.
- Making a reproduction of an intimate representation that the person knows or has reason to know was captured in violation of that prohibition, if the person depicted did not consent.
- Possessing, distributing, or exhibiting an intimate representation or reproduction made in violation of either of the above prohibitions, if the person has reason to know the intimate representation was captured or reproduced in such a way and the person depicted did not consent.

- Posting, publishing, or causing to be published a private representation (generally, a representation depicting nudity or sexual conduct that is intended by the person depicted to only be seen by certain persons) if the actor knows that the person depicted does not consent to the posting or publication of the private representation.
- Posting, publishing, or causing to be posted or published a depiction of a private representation, without the consent of the person depicted.

[s. [942.09](#), Stats.]

Breach of Personal Information

Under Wisconsin law, a business that holds personal information generally must notify consumers of any data breach that exposes that information. Personal information means a person's last name and first name or first initial, in combination with any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in such a manner that renders it unreadable: (1) Social Security number; (2) driver's license number or state identification number; (3) financial account number; (4) DNA profile; or (5) unique biometric data.

If a Wisconsin business entity knows that personal information in its possession has been acquired by a person whom the entity has not authorized to acquire the information, the entity must make reasonable efforts to notify each subject of the personal information. For an entity located outside of Wisconsin that possesses the personal information of a Wisconsin resident that is obtained by an unauthorized person, the entity must make reasonable efforts to notify each state resident who is the subject of the personal information. When notice is required, the entity must provide the notice within a reasonable time, not to exceed 45 days after it learns of the breach. Violations may be enforced by the Department of Agriculture, Trade, and Consumer Protection. [s. [134.98](#), Stats.]

Privacy

The statutes also recognize a right to privacy. Among the actions considered an invasion of privacy is the use, for advertising purposes or for purposes of trade, of the name, portrait, or picture of any living person, without having first obtained consent. A person whose privacy is unreasonably invaded is entitled to equitable relief, compensatory damages, and a reasonable amount for attorney fees. [s. [995.50](#), Stats.]

PART III | OTHER REGULATIONS RELATED TO AI

While certain specific uses of AI may be regulated by federal law, no comprehensive federal law regarding the use of AI has been enacted. Instead, federal regulations primarily address AI research and development, the coordination of AI policies within the government, and the implications of AI for national security. Several states have enacted legislation to regulate the use of AI. That legislation can be grouped in the following categories: the use of AI to generate sexual images, in political communications, and by state governments; the application of consumer and workplace protection laws to AI; and high-risk use of AI. In comparison, the European Union enacted broader AI legislation that classifies the uses of AI based on a tiered approach according to levels of risk.

FEDERAL GOVERNMENT

To date, Congress has not enacted comprehensive regulations regarding the use of AI. Congress has, however, enacted several bills that address AI, particularly related to the study of the use of AI and coordinating executive branch efforts related to AI.

National Artificial Intelligence Initiative Act of 2020

The National Artificial Intelligence Initiative Act of 2020 requires the President to establish and implement a national AI initiative to ensure continued U.S. leadership in AI research and development, lead the world in the development and use of trustworthy AI systems, prepare the workforce for the integration of AI systems across all sectors of the economy and society, and coordinate ongoing AI research, development, and demonstration activities across various agencies.

That legislation defines AI as the following:

[A] machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual systems. 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 U.S.C. s. 9401 (3).]

Among other provisions, it establishes a national AI initiative officer in the Office of Science and Technology Policy. That officer is required to establish an interagency committee to coordinate federal programs and activities in support of the AI initiative. The legislation also establishes a National AI Advisory Committee in the federal Department of Commerce to advise the President and Initiative Office on certain topics related to AI, and includes several provisions related to AI research. [[P.L. 116-283](#), Div. E.]

AI in Government Act of 2020

The AI in Government Act of 2020 created an AI Center of Excellence within the General Services Administration and tasks that body with certain duties, such as facilitating the adoption of AI in the federal government and improving cohesion and competency in the adoption and

use of AI within the federal government. It also requires the Director of the federal Office of Management and Budget (OMB) to issue memoranda to the head of each federal agency that addresses certain topics, such as recommending approaches to remove barriers for the use of AI in order to promote the innovative application of AI while protecting civil liberties, civil rights, and economic and national security, and identifying best practices for identifying, assessing, and mitigating any discriminatory impact or bias of any protected class from the use of AI. [[P.L. 116-260](#), ss. 101-105.]

Advancing American AI Act

The Advancing American AI Act was passed in December 2022. Among other provisions, it does the following:

- Requires the Secretary of the federal Department of Homeland Security to issue policies and procedures related to the acquisition and use of AI, and considerations for risks and impacts related to AI-enabled systems.
- Requires the Director of OMB to establish a work group to ensure that contracts for the acquisition of AI systems or services align with certain guidance and address issues such as protection of privacy, civil rights, and civil liberties.
- Requires the head of each agency to prepare and maintain an inventory of AI use cases, share agency inventories with other agencies, and make those inventories available to the public to the extent practicable.

[[P.L. 117-263](#), subtitle B.]

Executive Order 14110

On October 30, 2023, President Biden released an executive order titled, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Very generally, provisions in the executive order include the following: requiring developers of certain AI systems to share safety test results with the federal government; requiring the National Institute of Standards and Technology to establish standards related to the safety, security, and trustworthiness of AI systems; requiring the federal Department of Commerce to establish standards and best practices for detecting AI-generated content and authenticating official content; and issuing guidance for agencies to responsibly and effectively use AI. [[E.O. 14110](#).]

LEGISLATION REGULATING AI ENACTED IN OTHER STATES

Wisconsin is one of many states to enact legislation regulating the use of AI.¹⁸ States have most commonly enacted legislation to regulate the use of AI in generated sexual images, in political communications, and by state governments. Some states have also begun to enact regulations in the areas of consumer protection and

States have most commonly enacted legislation regulating the use of AI in political communications, in generated images, and by state governments. States vary widely in how they define concepts related to AI.

¹⁸ This overview of state regulations is based primarily on information compiled by the National Conference of State Legislatures (NCSL), relating to state regulation of AI. [NCSL, [Approaches to Regulating AI: A Primer](#), updated August 10, 2023; NCSL, [AI 2023 Legislation](#), updated January 12, 2024; and NCSL, [AI 2024 Legislation](#), updated June 3, 2024.] It is meant to provide a general survey of state regulations related to AI, but is not exhaustive.

criminal justice. Colorado’s legislation on high-risk AI use is credited as being the first comprehensive AI regulation in the country.¹⁹

AI and Generated Sexual Images

With recent technological advances, some states have updated their criminal codes to cover acts committed in ways not contemplated by prior law. For example, prohibitions on the nonconsensual distribution of certain kinds of images did not contemplate the possibility that a person could create images that appear to be of another person, but were actually computer-generated. Likewise, prohibitions on the possession of child pornography that is not deemed obscene generally require that the prohibited image be of an actual child.²⁰

Further, states must decide how to balance the desire to prohibit various kinds of offensive behavior with protections provided by the First Amendment. Both the U.S. and Wisconsin Constitutions generally prohibit the government from abridging the freedom of speech. While several categories of speech are not protected, statutes that regulate speech that does not fall into one of these categories of unprotected speech may be subject to challenge. For example, in the context of child pornography, the U.S. Supreme Court struck down two components of a federal statute that defined it to include images that were not of real children.²¹

Several states have enacted legislation related to AI and generated images that include nudity or sexual content. Some states have created criminal penalties, while others have created a civil cause of action.

Generated Sexual Images of Children

In addition to Wisconsin, at least eight other states have enacted legislation related to generated sexual images of children.

Similar to Wisconsin, Idaho and Oklahoma use an obscenity standard for certain images that appear to depict a child, but may not depict an actual child.²² Louisiana, Mississippi, and Utah amended their child pornography statutes to more generally include “morphed” or generated images.²³ Alabama, Florida, Kentucky, and Washington enacted new laws that consider whether the images appear to be of an identifiable child, would lead a reasonable person to believe the images are of a child, or are indistinguishable from a child.²⁴

South Dakota, in comparison, enacted a new law that considers whether the image depicts any of the following: (1) an actual minor that has been created, adapted, or modified to depict that minor engaged in a prohibited sexual act; (2) an actual adult that has been created, adapted, or

¹⁹ Seth Klamann, *Colorado passes first-in-US AI regulations*, *Denver Post*, May 24, 2024.

²⁰ See s. [948.12](#), Stats., and *New York v. Ferber*, 458 U.S. 747 (1982) (holding that child pornography may be prohibited even if not found to be obscene for several reasons, including the state’s compelling interest in safeguarding the well-being of minors involved in the production of such materials).

²¹ Very briefly, the U.S. Supreme Court held that two components of a federal statute’s definition of child pornography were overly broad and thus unconstitutionally burdened protected speech: a physical depiction that “is or appears to be” of a minor engaging in sexually explicit conduct and of any sexually explicit image that “conveys the impression” that it depicts a minor engaging in sexually explicit conduct. The Court held that this definition “proscribes a significant universe of speech that is neither obscene ... nor child pornography.” [*Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).]

²² [2024 Idaho House Bill 465](#) and [Oklahoma HB 3642](#). Idaho specifically refers to images created by generative AI or machine learning.

²³ For more detailed information, see: [2023 Louisiana Act 457](#); [2024 Mississippi House Bill 1126](#); and 2024 Utah House Bills [148](#) and [238](#).

²⁴ See: 2024 Alabama HB 168; [Florida Chapter No. 2024-118/Senate Bill 1680](#); [2024 Kentucky House Bill 207](#) and [Chapter 88, 2024 Washington Laws](#).

modified to depict that adult as a minor engaged in a prohibited sexual act; or (3) an individual indistinguishable from an actual minor created by the use of AI or other computer technology capable of processing and interpreting specific data inputs to create a visual depiction.²⁵

Other Generated Sexual Images

Several states have enacted legislation related to the nonconsensual distribution of generated sexual images. Some states, such as Alabama and California, prohibit any nonconsensual disclosure; while other states, such as Georgia, prohibit nonconsensual disclosure for certain purposes or when accompanied by certain harms. States that acted in this area generally enacted criminal prohibitions, though some states allow for a person depicted to bring a civil cause of action.

Alabama prohibits knowingly creating, recording, or altering a private image in which the person depicted had a reasonable expectation of privacy, without that person’s consent, including a recording that a reasonable person would believe actually depicts an identifiable individual, regardless of whether any portion of the recording is artificially generated. [[2024 Alabama HB 161](#).]

California created a civil cause of action for the nonconsensual, intentional disclosure of sexually explicit material of a depicted individual. A depicted individual is an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in an altered depiction. [[2019 California Assembly Bill 602](#).]

Georgia prohibits transmitting certain falsely created nude or sexually explicit videographic or still images. Generally, Georgia prohibits the knowing and nonconsensual electronic transmission of a photograph or video that depicts nudity or sexually explicit conduct, is harassment or causes financial loss to the depicted person, and serves no legitimate purpose to the depicted person. [[2019 Georgia Act 550](#).]

Hawaii prohibits intentionally creating, disclosing, or threatening to disclose an image or video of a composite, fictitious person who is depicted nude or engaged in sexual conduct, that includes the recognizable physical characteristics of a known person so that the image or video appears to depict the known person and not a composite, fictitious person, with the intent to substantially harm the depicted person in certain aspects of that person’s life. [[2021 Hawaii Act 59](#).]

Idaho prohibits knowingly distributing “explicit synthetic media” of an identifiable person, if the disclosure is made either without the consent of the person and would cause the person substantial emotional distress, or with the intent to annoy, terrify, threaten, intimidate, harass, offend, humiliate, or degrade the person. Explicit synthetic media is defined as any image or video that depicts or appears to depict an identifiable person engaging in sexual conduct that was created or altered using technical means, such as AI, to realistically misrepresent an identifiable individual as engaging in conduct in which the identifiable person did not engage. [[2024 Idaho House Bill 575](#).]

Illinois created a civil cause of action for the dissemination of an “intentionally digitally altered sexual image,” if the person depicted is identifiable to a reasonable person, suffers harm, and did not consent to the dissemination, and the actor knew or recklessly disregarded the possibility that the depicted individual did not consent, the image was an intentionally digitally altered sexual image, and the depicted individual was identifiable. [[Illinois Public Act 103-0294](#).]

²⁵ [2024 South Dakota Senate Bill 79](#).

Indiana prohibits knowingly distributing an “intimate image” that appears to depict an identifiable person without that person’s consent, including a computer-generated image, if the intimate image depicts nudity or sexual conduct, is created or modified by means of a computer software program, AI, application, or other editing tools, and is of a quality, characteristic, or condition such that it appears to depict the alleged victim. A computer-generated image is defined as a photograph, digital image, or video of an individual created or modified by means of a computer software program, AI, application, or other design editing tool. The prohibition is punishable by criminal penalties and a civil cause of action. [[2024 Indiana House Bill 1047.](#)]

Iowa prohibits the nonconsensual distribution of sexual images with intent to intimidate, annoy, or alarm, including images of an individual who is recognizable by his or her face, likeness, or other distinguishing features whose image is used to create, adapt, or modify a visual depiction. [[Iowa House Bill 2240.](#)]

Louisiana prohibits knowingly distributing “deepfakes” of another person engaging in sexual conduct without that person’s consent. A deepfake is defined as any audio or visual media in electronic format that is created, altered, or digitally manipulated in a manner that would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of the individual, or to falsely appear to replace an individual’s likeness with another individual depicted in the recording. A person who violates this prohibition is subject to criminal penalties. [[2023 Louisiana Act 457.](#)]

Minnesota prohibits the nonconsensual dissemination of a “deep fake” of an identifiable individual that realistically depicts nudity or certain sexual conduct, including artificially generated intimate parts presented as the intimate parts of the depicted individual. A deep fake is defined as a recording that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual, the production of which was substantially dependent upon technical means, rather than the ability of another person to physically or verbally impersonate such individual. Enforcement may be brought by both criminal penalties and a civil cause of action. [[Chapter 58, Minnesota Session Laws of 2023.](#)]

New York prohibits the intentional dissemination of an intimate image that depicts an identifiable person with exposed intimate parts or engaging in sexual conduct, including an image created or altered by digitization, with the intent to cause certain harms. Digitization means the alteration of an image in a realistic manner utilizing an image or images of a person, other than the person depicted, or computer-generated images. [[2023 Senate Bill S1042A.](#)]

Texas prohibits knowingly producing or distributing a deep fake video that appears to depict a person with the person’s intimate parts exposed or engaged in sexual conduct without that person’s consent. A deep fake video is a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality. [[2023 Texas SB 1361.](#)]

Virginia prohibits the unauthorized and malicious dissemination or sale of certain images of another person with the intent to coerce, harass, or intimidate, including a person 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. [[Chapter 490, 2019 Virginia Laws.](#)]

Washington prohibits the harmful and nonconsensual disclosure of a fabricated intimate image of another person. It also created a civil cause of action for the unauthorized disclosure, or threat of disclosure, of a fabricated intimate image. [[Chapter 88, 2024 Washington Laws.](#)]

Review of State Government Use of AI

At least 12 states have created advisory bodies to address issues related to the use of AI by state government. Very generally, these states require a state agency to inventory and assess ways in

which the state uses AI or require certain bodies to advise the state on the use of AI. California, in particular, requires an inventory of “high-risk automated decision systems” used by state agencies.

Alabama established the Alabama Council on Advanced Technology and AI, which is required to review and advise the Governor, the Alabama Legislature, and other interested parties on the use and development of advanced technology and AI in Alabama. [[Alabama Act No. 2021-344.](#)]

California requires the state Department of Technology to conduct a comprehensive inventory of all “high-risk automated decision systems” that have been proposed for use, development, or procurement by any state agency. The department must submit an annual report on its inventory to the California Legislature.

An automated decision system is a computational process that is derived from machine learning, statistical modeling, data analytics, or AI that issues a simplified output that materially impacts individuals by assisting or replacing human discretionary decision-making, with certain exceptions. An automated decision system is high-risk if it is used to assist or replace human discretionary decisions that have a legal or similarly significant effect, including decisions that impact access to or approval for housing, education, employment, credit, health care, and criminal justice. [[2023 California Assembly Bill 302.](#)]

Colorado created a Biometric Technology and AI Policy Task Force. Among other duties, the task force is required to propose policy recommendations related to key terms, such as “AI system;” develop recommendations related to algorithmic discrimination; and create a code of conduct or establish best practices for evaluating the ethical and equitable impact of using AI systems and automated decision systems. It provides that AI or an AI system means any machine-based system that, for any explicit or implicit objective, infers, from the inputs the system receives, how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments. [[Colorado H.B. 24-1468.](#)]

Connecticut requires its state Department of Administrative Services to inventory the use of AI by state agencies and perform ongoing assessments related to state use of AI to ensure that AI use does not result in unlawful discrimination or disparate impact. It also requires the state Office of Policy and Management to establish policies and procedures concerning the use and ongoing assessment of AI by state agencies. [[Connecticut Public Act No. 23-16.](#)]

It defines AI as either of the following:

- An artificial system that does any of the following: (1) performs tasks under varying and unpredictable circumstances without significant human oversight or can learn from experience and improve such performance when exposed to data sets; (2) is developed in any context, including, but not limited to, software or physical hardware, and solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; or (3) is designed to think or act like a human, or act rationally.
- A set of techniques, including machine learning, that is designed to approximate a cognitive task.

Florida created a Government Technology Modernization Council that is tasked with certain duties, including recommending legislative and administrative actions to promote the development of data modernization. [[Florida Chapter No. 2024-118/Senate Bill 1680.](#)]

Indiana enacted legislation that creates an AI task force to study and assess the use of AI technology by state agencies, allows political subdivisions and state agencies to adopt a technology resources policy and cybersecurity policies, and specifies requirements for entities that connect to Indiana’s state technology infrastructure. It defines AI as computing technology

that is capable of simulating human learning, reasoning, and deduction through certain processes, such as identifying patterns in data. [[2024 Indiana Senate Bill 150.](#)]

Maryland requires state agencies to conduct certain inventories and assessments of AI systems, and requires higher education institutions to establish policies on AI. It defines AI as a machine-based system that meets all of the following criteria: (1) can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments; (2) uses machine and human-based inputs to perceive real and virtual environments and abstracts those perceptions into models through analysis in an automated machine; and (3) uses model inference to formulate options for information or action. [[Maryland Senate Bill 818.](#)]

Oregon established a Task Force on AI. The task force is directed to examine and identify terms and definitions related to AI that are used in technology-related fields and may be used for legislation. [[2024 Oregon HB 4153.](#)]

Tennessee requires each public university, board of education, and public charter school to adopt a policy regarding the use of AI technology by students, faculty, and staff for instructional and assignment purposes. It defines AI to mean a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments and that is capable of using machine- and human-based inputs to perceive real or virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action. [[Tennessee SB 1711.](#)]

Texas created an AI Advisory Council that is tasked with studying and monitoring AI systems developed, employed, or used by state agencies, and to submit a report to the Texas Legislature on its findings. It also requires each state agency to submit an inventory of all automated decision systems being developed, employed, or procured by the agency.

It defines AI systems as systems that are capable of both of the following: (1) perceiving an environment through data acquisition and processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given a specific goal; and (2) learning and adapting behavior by analyzing how the environment is affected by prior actions. [[2023 Texas HB 2060.](#)]

Vermont created a Division of AI within its Agency of Digital Services. Among other duties, the Division of AI is required to review all aspects of AI developed, employed, or procured by the state; propose a state code of ethics related to AI; and conduct an inventory of all automated decision systems developed, employed, or procured by the state.

This Vermont law defines an AI system as a system capable of perceiving an environment through data acquisition, and then processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given a specific goal, and that can learn and adapt its behavior by analyzing how the environment is affected by prior actions. [[2021 Vermont Act 132.](#)]

West Virginia created a Task Force on AI that is tasked with certain responsibilities, such as recommending a definition of AI as it pertains to its use in technology for use in legislation, determining the relevant state agencies to develop and oversee AI policy, assessing the use of AI in the workforce, developing best practices for public sector uses of AI, and recommending legislation to protect individual rights, civil liberties, and consumer data as it relates to generative AI. [[2024 West Virginia House Bill 5690.](#)]

Use of AI in Political Communications

In addition to Wisconsin, several other states have enacted legislation that prohibits or requires disclosure of the use of AI in political campaign advertisements or election-related communications, though each state’s legislation differs in the scope of when those communications are prohibited or when disclosure is required.

Similar to Wisconsin Act 123, at least nine states have enacted laws that generally require disclosures when political communications include material that is produced by generative AI or contains “synthetic media.” Those states are the following: Alabama, Arizona, Michigan, Mississippi, New Mexico, New York, Oregon, Utah, and Washington. California and Florida enacted requirements that apply to communications that have been manipulated or use generative AI to falsely appear to depict a person performing an action that did not occur in reality. At least three states, Idaho, Michigan, and Minnesota, prohibit the use of certain AI-generated media in political communications in certain circumstances, regardless of whether the communication includes a disclosure.²⁶

In comparison, **Arizona** allows a candidate for public office to sue for injunctive relief in certain circumstances where a “digital impersonation” of the candidate has been published without the candidate’s consent and the publisher did not take reasonable steps to disclose that the recording or image was a “digital impersonation.” [[Arizona HB 2394.](#)]

Consumer and Workplace Protection

At least six states have enacted legislation to address AI in the field of consumer or workplace protection.

California prohibits the use of a bot to communicate or interact online with another person with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication to incentivize a purchase or sale of goods or services, or to influence an election. A “bot” is an automated online account where all or substantially all of the actions or posts of that account are not the result of a person. [[2017 California Senate Bill 1001.](#)]

Colorado prohibits an insurer from using any external consumer data or information sources, including algorithms and predictive models, to unfairly discriminate based on certain protected classes, such as race, sex, and sexual orientation. [[Colorado Senate Bill 21-169.](#)]

Illinois created a Generative AI and Natural Language Processing Task Force, which is required to investigate and provide a report on generative AI software and natural language processing software. The task force has certain duties, such as recommending legislation or regulations to protect consumer information as it relates to AI and recommending model policies for schools to address the use of generative AI by students. It does not define AI or natural language processing. [[Illinois Public Act 103-0451.](#)] Illinois also requires that an employer notify job applicants before a videotaped interview if AI may be used to analyze the interview and consider the applicant’s fitness for the position. It also requires the employer to explain how AI may be used and to obtain consent from the applicant to be evaluated with the AI program. [[Illinois Public Act 101-260.](#)]

²⁶ For detailed information, see the following: Alabama HB 172; Arizona HB 2394; [2019 California Assembly Bill 730](#); [Florida Chapter No. 2024-126/House Bill 919](#); [Idaho House Bill 664](#); Michigan 2023 Public Acts [263](#), [264](#), [265](#), and [266](#); [Chapter 58, Minnesota Session Laws of 2023](#); Mississippi SB 2577; [2024 New Mexico House Bill 182](#); New York AB8808, subpart B; [2024 Oregon SB 1571](#); [Utah S.B. 131](#); and [Chapter 360, 2023 Washington Laws](#).

Tennessee provides that an individual has a property right in the use of his or her voice, name, photograph, or likeness, and that right is exclusive to the individual. Likewise, it prohibits the unauthorized use of a person's voice for certain commercial purposes without the individual's consent. A person whose property right has been infringed upon may bring a civil action against any person who knowingly uses or infringes upon the person's property right or distributes an algorithm or other technology, if the primary function of the algorithm or other technology is to produce a particular person's photograph, voice, or likeness, with knowledge that distributing the person's photograph, voice, or likeness was not authorized. [[2024 Tennessee Public Chapter No. 588.](#)]

Utah created an Office of AI Policy and a regulatory AI analysis program and established liability for the use of AI that violates consumer protection laws if not properly disclosed. The state also requires disclosure when a person interacts with AI when engaging with state-licensed or state-certified occupations. [[Utah S.B. 149.](#)]

Use of AI in Law Enforcement

Several states have enacted restrictions on the use of facial recognition technology by law enforcement agencies. For example, **Virginia** creates a state mechanism for determining which uses of facial recognition technology a law enforcement agency is authorized to use under state law. The state also creates restrictions on the manner in which facial recognition technology may be used to show probable cause for the issuance of a search or arrest warrant. [[Chapter 737, 2022 Virginia Laws.](#)] **Washington** prohibits the use of facial recognition technology by a state or local government agency based on their religious, political, or social views, or actual or perceived race, ethnicity, or citizenship, among other criteria. The state also prohibits a state or local government agency from using facial recognition technology while engaging in certain surveillance activities without a warrant, unless an exception applies. [[Chapter 257, 2020 Washington Laws.](#)]

Use of AI in the Criminal Justice System

California requires that each pretrial services agency that uses a pretrial risk assessment tool validates that tool at least every three years and makes certain information regarding the tool publicly available. [[2019 California SB 36.](#)]

Utah prohibits a court from solely using an algorithm or risk assessment tool score in determining whether a criminal defendant should be diverted to a noncriminal diversion program or determining the appropriate sentence for a criminal defendant. [[Utah H.B. 366.](#)]

Regulation of High-Risk AI Use

As was mentioned, **Colorado** has been described as the first state to comprehensively regulate the use of AI. Colorado's legislation, which is similar to that introduced in several other states, primarily regulates developers and deployers of high-risk AI systems and focuses on the high-risk use of AI. A high-risk AI system is an AI system that, when deployed, makes (or is a substantial factor in making) a consequential decision, with certain exceptions. Examples of consequential decisions include those that have a material legal effect on the provision, cost, or terms of an education or employment opportunity, housing, or an essential government service.²⁷

²⁷ Colorado's legislation defines an AI system using the OECD definition.

Colorado's legislation generally does all of the following:

- Requires a developer of a high-risk AI system to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination that may arise from uses of the AI system. There is a rebuttable presumption of reasonable care for a developer that complies with the law and follows certain requirements, such as making available a general statement describing the reasonably foreseeable uses and known or inappropriate uses of the high-risk AI system and summaries of the type of data used to train the system.
- Requires a deployer of a high-risk AI system to do all of the following:
 - Use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination.
 - Implement a risk management policy and program to govern the deployer's use of a high-risk AI system, which must specify and incorporate the principles, processes, and risks used to identify, document, and mitigate known or reasonably foreseeable risks of algorithmic discrimination.
 - Complete an impact assessment at least annually and after any modification to the high-risk AI system. The impact assessment must include information such as an analysis of whether the deployment of the high-risk AI system poses any known or reasonably foreseeable risks of algorithmic discrimination and the steps taken to mitigate those risks.
 - Notify consumers when a deployer uses a high-risk AI system to make, or be a substantial factor in making a consequential decision concerning the consumer.
 - Make available on its website a statement summarizing certain information regarding the deployer's use of any high-risk AI system.
 - Disclose to a consumer that interacts with an AI system that is intended to interact with consumers.
 - Provide notice to the Colorado Attorney General of any discovery of algorithmic discrimination caused by a high-risk AI system.

A violation of the legislation is considered an unfair trade practice and may be prosecuted by Colorado's Attorney General. The legislation takes effect in 2026. [[Colorado SB24-205.](#)]

EUROPEAN UNION

The European Union recently adopted the AI Act, which utilizes a risk-based approach to AI regulation. It classifies AI systems in four categories based on the level of risk presented, from minimal risk to unacceptable risk, with requirements dependent on the AI system's classification. For example, high-risk AI systems must satisfy certain requirements, such as establishing a risk management system that identifies and analyzes potential risks to health, safety, or fundamental rights; estimates and evaluates those risks; and adopts measures to manage those risks. It defines an AI system in a manner similar to the OECD.²⁸

²⁸ Specifically, the AI Act defines an AI system as a machine-based system designed to operate with varying levels of autonomy, 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. [[AI Act](#) art 3, s. (1) and arts. 8-17.] See also European Commission, [AI Act](#) (accessed July 15, 2024).