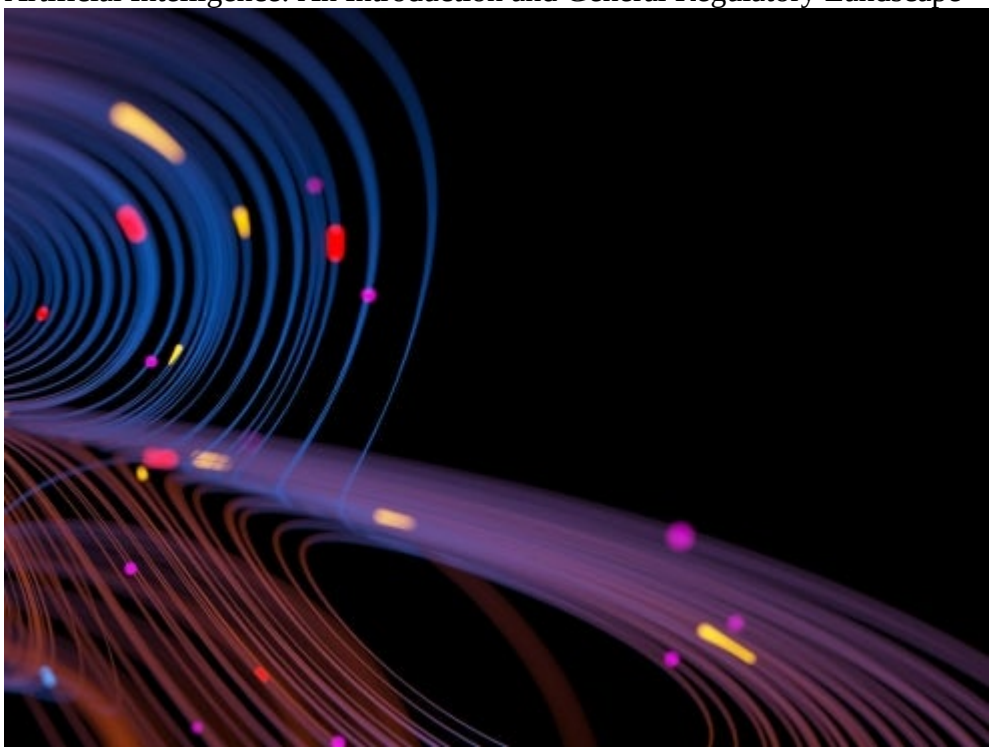
Blogs
August 04, 2023
Artificial Intelligence: An Introduction and General Regulatory Landscape



Introduction to AI and Definitions

Artificial intelligence (AI), a term first coined in the 1950s, is a field of technology that engages in problem-solving by using AI algorithms to make predictions or classifications based on input data.[1] With the recent emergence of generative AI technology, the regulation of AI has become a priority for various governmental agencies due to its expansive capabilities and potential uses. As AI technology continues to develop and be used across industries, investment managers, developers, and regulators alike must consider the implications and risks associated with using this technology.

This series of articles will discuss the potential regulation of AI technology in the financial services industry. This article will begin the series with a discussion of the general regulatory landscape of AI in the United States.

While many definitions of AI exist, a popular definition of AI is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.[2] Different types of AI exist, including weak AI, strong AI, deep learning, and machine learning (ML).[3] Weak AI, also referred to as narrow AI, is the most common AI used today and is AI trained to perform specific tasks. It is used in popular speech recognition virtual assistants and autonomous cars.[4] Strong AI is based on the Turing test, in which a machine would have the intelligence equal to that of a human or exceeds the intelligence of a human, respectively.[5]

ML is a subfield of AI and involves training algorithms on large datasets to identify patterns and relationships and then using these patterns to make predictions or decisions about new data.[6] Deep learning is a subfield of ML and is composed of neural networks with multiple layers that are used to analyze complex patterns and relationships in data, thereby enabling the use of larger data sets.[7]

Generative AI refers to deep-learning models that can learn to generate new outputs based on the data they have been trained on.[8] Generative models can create new content in the form of images, text, and audio.[9] Deep-

learning AI models will soon outpace or replace narrow AI models as they can work across broad domains and solve an array of problems.[10]

With more industries exploring or beginning to incorporate AI into their operations and the developing capabilities of AI models, government bodies and corporations alike have voiced their concerns about the potential risks and ethical implications of AI.

Innovation

The U.S. government has yet to pass any comprehensive legislation regulating the development and use of AI in enterprise. The limited legislation passed and regulatory guidelines issued by government agencies, particularly throughout 2020, suggested that the federal government was committed to encouraging the innovation of AI technology. In 2020, a memo issued by the Office of Management and Budget encouraged federal agencies to avoid passing regulations or taking nonregulatory action that would interfere with AI innovation or growth.[11] The memo reasoned that the innovation and growth of AI is important because it "holds the promise to improve efficiency, effectiveness, safety, fairness, welfare, transparency, and other economic and social goals, and America's continued status as a global leader in AI development is important to preserving our economic and national security."[12]

The legislation passed to date by Congress concerning AI has encouraged the use and development of AI technology. For example, the AI in Government Act of 2020 "establishes the AI Center of Excellence to facilitate and coordinate federal government adoption of AI technologies."[13] The National AI Initiative Act of 2020 "sets forth policies regarding certain federal activities related to artificial intelligence, including implementation by the president of a National Artificial Intelligence Initiative to support research and development, education, and training programs."[14] Finally, the Advancing American AI Act seeks to "encourage agency artificial intelligence-related programs and initiatives that enhance the competitiveness of the United States in innovation and entrepreneurialism" and "enhance the ability of the Federal Government to translate research advances into artificial intelligence applications to modernize systems and assist agency leaders in fulfilling their missions."[15]

The National Artificial Intelligence Initiative Office (NAIIO), established in the National AI Initiative Act of 2020, has released ways in which federal agencies are incorporating the use of AI into their operations.[16] With respect to financial services, the U.S. Department of the Treasury and the Securities and Exchange Commission (SEC) are adopting AI technology and machine learning.[17] The SEC, in particular, is implementing machine learning algorithms to monitor and detect potential investment market misconduct.[18]

As AI technology has developed and been implemented across industries, it is evident there are risks associated with its use, and there has been a shift this year towards understanding how best to regulate AI while still promoting innovation. Although very little legislation regulating AI technology has passed, it is likely that more comprehensive legislation will be passed in the future as members of Congress continue to educate themselves on the potential uses and risks of AI technology. Senator Chuck Schumer recently announced his SAFE Innovation Framework for AI Policy, a two-step plan to regulate AI technology.[19] The first step in the plan establishes a framework for action that encourages innovation while calling for security, accountability, protecting democratic foundations, and explainability.[20] The second step in the plan outlines Congress' approach to creating legislation. In the fall of 2023, members of Congress will host a series of AI insight forums, hearing from AI developers, executives, scientists, advocates, and others to further their understanding of AI technology and lay the groundwork for creating AI policy.[21] The House Energy and Commerce Committee approved the AI Accountability Act in mid-July and will send the bill for a possible vote on the House floor in the fall. The AI Accountability Act would direct the Assistant Secretary of Commerce for Communications and Information to conduct a study and hold public meetings with respect to artificial intelligence systems.[22] In the

Senate, there is a proposal for the AI LEAD Act, which would establish the Chief Artificial Intelligence Officers Council, Chief Artificial Intelligence Officers, and Artificial Intelligence Governance Boards.[23]

Risks and Risk Management

The primary risks associated with AI that federal agencies have identified are safety, risks to democratic values, and risks to privacy.[24] AI Algorithms can be biased and can discriminate against a protected class. For example, many industries use AI in the hiring process. Evidence shows that input data used in these algorithms can lead to biased outcomes in hiring.[25] For example, biased AI algorithms could have significant negative implications for companies seeking to increase diversity in their hiring practices or comply with specific ESG standards.

In addition to the risk of AI technology infringing on democratic values, the use of AI systems presents risks to users' privacy. Given the importance of data in AI algorithms making predictions, AI models may engage in abusive data practices and using and storing data without the consent of the user.[26] AI algorithms could prove to be a particular risk to investors and fund managers because many corporations use AI models developed by third parties. Therefore, confidential data could be compromised and exposed to third parties when input into an AI algorithm.

While the federal government has yet to take legislative action against the potential risks associated with the use of AI technology, federal agencies have issued guidelines on how to mitigate potential risks. As AI continues to be developed and used in ways that it hasn't been before, the risk of using AI for harm, whether intended or not, increases.

Biden Administration

The Biden administration has published an AI Bill of Rights to offer guidance on how AI should be developed and used to be safe and effective without infringing on civil rights.[27] The AI Bill of Rights suggests that AI systems should be developed with consultation from diverse communities and consider the potential impact on diverse users and communities in general.[28] To ensure risks are minimized, the AI Bill of Rights recommends that AI systems undergo pre-deployment testing, risk identification and mitigation, ongoing monitoring, mitigation of unsafe outcomes, including those beyond the intended use, and adherence to domain-specific standards.[29]

The pre-deployment testing suggested in the AI Bill of Rights recommends following domain-specific best practices and mirroring the conditions in which the technology will be employed to ensure the technology will work in its real-world context.[30] The testing should account for both the AI technology and the role of human operators who may affect system outcomes.[31] The AI Bill of Rights suggests that developers of AI systems identify potential risks of the system, both before and during the system's deployment. Mitigation of the potential risks should be proportionate to the level of risk identified, and systems should not be used until risk can be mitigated.[32] AI systems should be designed to proactively protect users from harm stemming from both intended and unintended, yet foreseeable uses or impacts of the AI system.[33]

To protect users against abusive data practices, the AI Bill of Rights suggests that AI developers create built-in protections and give users agency over how their data is used.[34] AI developers should seek users' permission and should limit the data collected to only that which is strictly necessary for the specific context in which it is collected.[35] For AI system users to have agency over how their data is used, they should receive notice and an explanation that an AI system is being used. The AI Bill of Rights encourages developers to provide plain language documentation of the AI system being used and a clear description of its role.[36] The explanations should be technically valid, meaningful, and useful to the user and others who may need to understand the

system.[37]

Finally, the AI Bill of Rights suggests that AI systems should have human alternatives to fall back on if the system experiences unintended problems.[38] Human alternatives should give users the ability to opt out of the AI system, where appropriate, and give them access to a human operator who can assist with and remedy any issues, such as a system error or failure.[39] The appropriateness of opting out is determined by reasonable expectations within the context and focuses on ensuring broad accessibility and protecting the public from especially harmful impacts.[40]

The Biden administration is also working with several AI companies, and this July, received voluntary commitments from seven companies to move toward safe, secure, and transparent development of AI technology. The voluntary commitments include testing the safety and capabilities of the AI systems, ensuring that the technology does not promote bias and discrimination, strengthening privacy protections, and shielding children from harm.[41]

While the federal government has been relatively hands off to date in regulating the development and use of AI technology, the use of AI can pose certain risks and may have regulatory implications on the financial services industry.

The next article in this series will discuss the SEC's proposed regulation of AI technology.

The author wishes to acknowledge the contributions of summer associate Stephanie Flynn.

---

[1] *What is Artificial Intelligence (AI)?*, IBM (2023).

[2] Chethan Kumar, *Artificial Intelligence: Definition, Types, Examples, Technologies*, Medium (Aug. 31, 2018).

[3] IBM, *supra* note 1.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] Scott W. Bauguess, Acting Director and Acting Chief Economist, DERA, The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective (June 21, 2017),.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Off. Of Mgmt. & Budget, Exec. Off. Of the President, M-21-06, Guidance for Regulation of Artificial Intelligence Applications (Nov. 17, 2020).

[12] *Id.*

[13] AI in Government Act, H.R. 2575, 116th Cong. (2020) (incorporated in H.R. Con. Res. 133, 116th Cong. (2020) (enacted)).

[14] National AI Initiative Act of 2020, H.R. 6216, 116th Cong. (2020).

[15] Advancing AI Research Act of 2020, S. 3891, 116th Cong. (2020).

[16] *ld.*

[17] *Id.*

[18] *Id. See* Bauguess, *supra* note 7.

[19] Schumer, *supra* note 11.

[20] *Id.*

[21] *Id.*

[22] *ld.*

[23] *ld.*

[24] Off. Of Sci. And Tech. Pol'y, Exec. Off. Of the President, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *From Principles to Practice: A Technical Companion to the Blueprint for an AI Bill of Rights*, The White House (Oct. 2022).

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Off. Of Sci. And Tech. Pol'y, *supra* note 21.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] https://www.whitehouse.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf

Explore more in

Investment Management