

The Investment Lawyer

Covering Legal and Regulatory Issues of Asset Management

VOL. 30, NO. 11 • NOVEMBER 2023

Thinking About AI—Considerations for Boards of Directors

By Molly Moynihan and Sandhya Ganapathy

Since the public launch of ChatGPT in November 2022,¹ artificial intelligence (AI) has become the latest new technology craze. While chatbots are certainly fun to play with, hallucinations and all, many directors are seeking to understand how, if at all, this technology will impact the day-to-day operations of the funds they oversee. This article seeks to demystify AI, through providing a brief primer on the topic. It then discusses (1) applications for AI in our industry, (2) the regulatory framework surrounding AI, and (3) considerations for directors in overseeing funds and advisers as AI is deployed across the industry.

AI Primer

Artificial intelligence, a term invented in the 1950s, is itself a rather fluid concept. John McCarthy, who many consider the father of AI, defined it as, “[G]etting a computer to do things which, when done by people, are said to involve intelligence.”² The National Institute of Standards and Technology (NIST) has defined AI as “[S]oftware and/or hardware that can learn to solve complex problems, ... solve tasks that require human-like sensing..., cognition, planning, learning, communication, or physical action”³ And IBM has suggested that, “At its simplest form, artificial intelligence is a field, which combines computer science and robust datasets, to enable problem-solving.”⁴

The critical thing to know is that, despite the hype, AI does not think, and it does not know. It involves a system of immensely complex pattern recognition that is performed by a machine. ChatGPT, for example, uses “a type of neural network known as a transformer. Transformers are a type of deep learning algorithm that is commonly used in the field of natural language processing (NLP). They are designed to process sequences of data, such as text, and learn patterns in that data that can be used for various NLP tasks, such as text generation or question answering.”⁵ The system can thus access a vast bank of data and predictively generate “contextually relevant responses.” The AI involved in these systems can generate true information (that is, “get it right”), but it can equally generate information that may be contextually relevant and yet flat out wrong.

While chatbots, a more accessible form of AI, represent a step change in the public’s understanding of AI, many AI-based applications have been with us for years. In recent remarks on AI, US Securities and Exchange Commission (SEC) Chair Gensler observed that artificial intelligence technology “already is playing a part in call centers, account openings, compliance programs, trading algorithms, sentiment analysis, robo-advisors, and brokerage apps.”⁶ Common applications, as discussed below, with which most are already familiar, include digital assistants, navigation apps and driver assistance features on vehicles.

Types of AI

There are distinct types of AI, including weak AI, strong AI, and the related subfields of deep learning, machine learning (ML), and generative AI. Weak AI, also referred to as narrow AI, is the most common AI used today and consists of AI trained to perform specific tasks, for example, a navigation app, as described above, or automated responses utilized by a call center. Strong AI represents the wave of the future, in which AI's capabilities are more generalized.

Machine learning is a subfield of AI which involves the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.

Deep Learning is a type of ML that uses artificial neural networks made up of many interconnected nodes to process more complex patterns using larger data sets than traditional ML. Although the technology borrows vocabulary used to describe the human brain, so-called neural networks are actually complex pieces of code—no neurons involved. The coding, however, is designed to replicate the complex relationships within the human brain that allow for pattern recognition, prediction and inference. In an artificial neural network, there is an input layer, one or more hidden layers, and an output layer. Based on various parameters, each node connects to another and under certain conditions can send data to the next layer of the network, ultimately yielding the output. Neural networks can be trained on large data sets to learn and improve their accuracy over time. Their strength is that once trained they classify and cluster data at a high velocity.⁷ This is the superpower of AI, because it allows data to be classified and summarized almost instantaneously when compared to the time required for humans. Search algorithms that can search the web in an instant to deliver useful information on everything from local restaurants to physics are an example of the power of neural networks.⁸

Large language models (LLM) are very large, complex deep learning models that are trained on massively large datasets. LLMs can “understand” text to help them summarize, generate and predict new content. Generative AI, such as ChatGPT, refers to deep learning models that can learn to generate new outputs based on the data they have been trained on. Rather than identifying existing information, like a search engine, generative models can create new content in the form of images, text, and audio.

Parameters are an overlooked, but key point in understanding how deep learning AI works. Simply put, parameters are the variables in a deep learning model that can be adjusted to influence the model's performance. They control, in effect, the conditions under which the different nodes will connect with each other. Generally, parameters are connection weights and biases. For example, they can be weights in the connections between nodes, or with respect to the thresholds for creating a connection among nodes. Examples of parameters include things like pixels or color depth when using AI to identify objects in images. In that case, parameters that represent the weights of the connections between pixels and what causes a node to send data would be important.

The programming capacity to use enormous numbers of parameters has been a key driver in the increasing abilities of AI. For example, in 2018, the first version of ChatGPT was trained on 120 million parameters. The most recent version of ChatGPT, released in 2022, was trained on in excess of 100 trillion parameters.⁹ However, while the ability to add parameters vastly increases the power of AI, it should be noted that the addition of parameters adds significant cost to the development of LLMs. The ability to train LLMs on huge data sets has been a major driver in the development of the technology. And it sheds light on why all of this is possible now. The Internet has been around since January 1, 1983. Google launched on September 4, 1998. In the past 40 years greater and greater amounts of data have been generated digitally. The amount of data available today

combined with available computer processing power now roughly correlates to the amount of data needed to effectively deploy LLMs.

As the capabilities of AI increase, experts across all industries are asking themselves how they can benefit from AI and what threats it poses. It has been estimated that in the next decade, nearly one-fourth of all tasks currently performed by US workers and 35 percent of those performed in the financial services industry could be performed by AI enhanced bots.¹⁰ On the other hand, most experts also believe that while AI has the capacity to reduce mundane and rote tasks such as the gathering and summarizing of data, human expertise will continue to be an essential feature of any workstream. So, while it may be possible to use AI to summarize financial data or assist with first drafts of performance reports and financial statements, execute trading strategies, field routine calls in a call center, review email for spam, or perform routine compliance reviews, the output will still require expert review by knowledgeable humans.

Challenges to AI Models

AI models, however, in their current form, present multiple challenges. Two examples relate to model drift and model collapse. With respect to both, an AI model is only as good as the data it is trained on and the more heterogenous the data, the better the model. In 2022, however, almost half of the content on the Internet was generated by bots.¹¹ If the data on which an AI model is trained is homogenized or otherwise defective, the model can collapse. For example, it was originally thought that AI could eliminate bias since a machine should not be biased, but researchers quickly discovered that was not true, because the training data was itself biased. Similarly, while a model may be set with specific parameters, it may for reasons not completely understood, drift over time, such that the outputs differ from those intended by the trainers. For this reason, as discussed below, testing both before deployment and once deployed is an essential

component of using AI. Testing allows an enterprise to evaluate outputs, compare them against expectations and then build constraints to limit permissible drift.

Applications in Financial Services and the Mutual Fund Industry

AI has already been broadly deployed across the financial services industry. It can be as simple as an analyst using AI to quickly generate code, to its use to identify trends in data, to summarize fund performance, to detect fraud, or to design and implement portfolio management strategies and the use of robo-advisers. One of the most attractive features of this technology is that it speeds up time to market, and in financial markets, speed can be important. AI models can rapidly summarize earnings data, financial reports, and other more arcane market data to generate and in some cases execute buy and sell recommendations. In some marketing efforts, wholesalers can reach out to multiple clients, and the first interactions will be with an AI enhanced machine, until there is a level of interest that justifies a human interaction. AI can also be used to analyze browsing patterns to identify when a customer might be ready to invest, speeding up the efficiency of the sales cycle. On the transfer agent side, AI can be used to spot fraud through its ability to detect anomalous patterns in data. On the other hand, AI can be used to commit fraud more effectively, because bad actors can use it to detect how defenses operate and to circumvent those defenses.

The trading capabilities of AI already have been utilized for some time by both quant-based managers and active managers who use the ability of machine learning to rapidly digest market data.¹² Some hedge funds using these technologies have achieved excellent performance. Renaissance Technologies' Medallion Fund, which uses quantitative trading techniques fed by massive data sets and rules-based algorithmic trading returned 66 percent on an annualized basis before fees and 39 percent after fees from

1988 to 2018.¹³ Multiple asset managers are engaged in pilot programs.¹⁴ Several AI driven exchange-traded funds (ETFs) also have been launched.¹⁵ Kaiju ETF Advisors developed the first actively managed ETF in which the AI itself executes the trades.¹⁶ ETFMG's AI Powered Equity ETF (AIEQ)¹⁷ and the Qraft AI-Pilot US Large Cap Dynamic Beta and Income ETF (AIDB)¹⁸ currently use AI to make all fund investment decisions. Ocean Capital Advisors, in partnership with ETFMG has launched Rogers AI Global Macro ETF, a global macro ETF of ETFs, which is the first passive artificial intelligence backed ETF that uses AI to determine every investment decision and reveal the specific processes behind each decision.¹⁹

AI is being used to increase efficiency on the administrative side of the fund space by sifting through vast amounts of internal communications, assisting with document review, creating financial literacy documents and web content, and reviewing and approving public communications. AI-enhanced document generation can also be used by legal and accounting departments and improved speech recognition and generation can improve call center functioning. Implications for AI in the cybersecurity space are mixed. AI's ability to adaptively learn and detect novel patterns can both accelerate detection, containment, and response, and create enhanced opportunities for spoofing, phishing, and other fraud.

Regulatory Framework

Regulators around the globe are scrambling to deal with the complex challenges posed by AI. Issues that are not unique to the financial services industry include: bias, intellectual property, and privacy. Each of these is discussed below.

AI algorithms can be biased if the input data or underlying model, created by humans, is biased.²⁰ For example, the real world exhibits long-standing patterns of bias and discrimination, this data then forms the basis for training the AI (including for example data sets that represent sampling bias),

the design of the model itself may involve unrecognized bias, and the outputs may reinforce the bias embedded in the data. As a result, the use of AI programs has been shown to result, for example, in biased hiring and healthcare practices. In response, New York City²¹ recently has passed and implemented laws requiring AI hiring programs and healthcare algorithms to be audited for bias before use.

The creation of AI models involves scraping data from the web. In so doing, protected intellectual property may be infringed upon. Lawsuits have been filed against AI platforms by creators who claim AI is using their original works without their permission to train AI in their styles in which plaintiffs have claimed copyright infringement,²² trademark infringement,²³ right of publicity misappropriation,²⁴ and raised interesting and novel questions with respect to ownership of outputs.²⁵ Another interesting issue relates to data input by users of ChatGPT and other chatbots. In that case, the AI model may use the data, including the search terms themselves, input by the user to train on. Confidential information could thus be compromised. For this reason, many enterprises have limited the use of chatbots and other AI tools.

With respect to privacy, AI algorithms may engage in abusive data practices because they rely on input data to learn and predict patterns. Therefore, AI algorithms may store user data without the consent of the user. Many individuals also have discovered that chatbots generate misinformation concerning themselves or others. For this reason, the Federal Trade Commission has opened an investigation over whether a chatbot has harmed consumers through its collection of data and its publication of false information on individuals.²⁶ Because personal identifiable information (PII) maintained by asset managers is generally carefully protected already, this should not pose an issue for asset management firms, although individual portfolio managers or directors may be surprised by the information generated by chatbots.

European Union AI Act

The European Union AI Act²⁷ provides a useful framework for thinking about AI risk. It essentially creates a risk pyramid and regulates activity according to its risk classification. At the top is social scoring, mass surveillance, and manipulation of behavior causing harm, which are categorized as unacceptable risk and strictly prohibited. Next, access to employment, education and public services, safety components of vehicles, and law enforcement are categorized as high risk and regulated to require conformity with identified standards. Impersonation, chatbots, emotion recognition, biometric categorization and deep fakes are categorized as limited risk, and require transparency and disclosure to make clear that AI is being used. All remaining applications are considered minimal risk and no regulations are applied.

Biden Administration AI Bill of Rights

Although Congress has yet to act, the Biden administration issued a so-called Blueprint for an AI Bill of Rights in October 2022,²⁸ which contains a set of “five principles and associated practices” to help “guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence.”²⁹ The AI Bill of Rights provides for the following:³⁰

1. *Safe and Effective Systems.* Systems should be designed to proactively protect users from harms stemming from unintended, yet foreseeable, uses or impacts of automated systems.
2. *Algorithmic Discrimination Protections.* Algorithms should be free from discrimination and systems should be used and designed in an equitable way,
3. *Data Privacy.* Users should have agency over how their data is used, and systems should have built-in protections against abusive data practices,
4. *Notice and Explanation.* Developers should provide a plain language, easily understandable description of the system.

5. *Human Alternatives, Consideration, and Fallback.* Users should be able to opt out and have access to a person who can remedy problems.

Securities and Exchange Commission Concerns—Generally

Chair Gensler has been active in speaking on the topic of AI.³¹ The concerns raised by Chair Gensler and SEC Staff concern the following topics:

1. *Conflicts of Interest.* This concern pertains to the concern that when brokers and financial advisors utilize AI to service a client, they still owe a fiduciary duty to that client. There is thus concern over whether the AI being used is optimizing in favor of the client’s best interests, or in favor of the brokers’ and financial advisors’ best interests. This in turn can be related to the parameters that are built into the AI model which guide the interests that the model seeks to optimize—that is, make money for the adviser or make money for the client. The nuances associated with fiduciary principles are complex to build into an AI model.³²
2. *Digital engagement practices.* Use of predictive data analytics, built upon artificial intelligence and machine learning, coupled with differential marketing, differential pricing, and individually tailored behavioral prompts—what the SEC calls digital engagement practices—raise suitability and best interest concerns. For example, while it may be appropriate for Tik Tok to endlessly serve up video that is algorithmically designed to stimulate engagement, regulated entities must build in safeguards to ensure that the content generated for clients meets regulatory requirements.³³
3. *Bias and Misinformation.* AI developers need to be conscious in disallowing their programs from accessing data that reinforces historical inequities and reflects bias. There is concern over AI’s ability to enable fraud and spread misinformation.
4. *Systemic and Market Risk.* Too much concentration among AI programs could leave the financial

system vulnerable. Specifically, the programs could pose a systemic risk if there is too much concentration among AI data aggregators and generative AI and one of the programs makes an error. Similarly, reliance on a small number of vendors in the generative AI level of a tech stack with multiple fintech applications built on top of that level could result in cascading failures.³⁴ In addition, markets already have experienced flash crashes and other impacts of increasingly sophisticated algorithmic trading. The ability to generate deep fakes also has the potential to impact markets. For example, in May 2023, a fake image of an explosion near the Pentagon was shared on Twitter leading to a brief dip in the stock market.³⁵

5. *Accountability.* As algorithms learn and move farther from their initial programming, who should be held accountable if it makes an error? This is a rapidly growing concern that AI developers and providers will need to address, and which should be controlled through design, governance, and initial and ongoing testing of AI models.³⁶
6. *Explainability.* Explainability is the ability to express why an AI system reached a particular decision, recommendation, or prediction. Developing this capability requires understanding how the AI model operates and the types of data used to train it, which may become difficult as the model iterates. Again, robust testing to ensure that outputs remain consistent with expectations is essential to maintain explainability.³⁷

SEC proposed AI Conflicts of Interest Rule

As a first step in addressing these issues, on July 26, 2023, the SEC proposed new rules under the Securities Exchange Act of 1934 (Exchange Act) and the Investment Advisers Act of 1940 (Advisers Act) that would require broker-dealers and investment advisers, registered or required to be registered under Section 203 of the Advisers Act, to take certain steps to address conflicts of interest associated with their use of predictive data analytics and similar

technologies (the AI Conflicts of Interest Rule).³⁸ The proposed rule would require broker dealers and advisers to eliminate or neutralize the effect of conflicts of interest associated with the firm's use of technologies³⁹ that optimize for, predict, guide, forecast, or direct investment-related behaviors that result in investor interactions that place the interest of the firm or its associated persons ahead of investors' interests (whether intentionally or unintentionally).

Under the proposed rules, firms must evaluate the use of covered technologies to identify conflicts, eliminate or neutralize the effect of the conflicts once identified, and adopt written policies and procedures reasonably designed to prevent violations and achieve compliance with the proposed rules.⁴⁰ The firms must also review, no less frequently than annually, the adequacy of the policies and procedures established pursuant to the proposed rules and the effectiveness of their implementation.⁴¹ Importantly, the AI Conflicts of Interest Rule also requires firms to test a covered technology prior to its implementation or material modification and periodically thereafter to determine whether it could give rise to a conflict of interest.⁴²

Board Considerations

As boards of directors seek to come to terms with the implications of use of AI for their oversight duties, a useful adage is "Build the brakes when you build the car!" This technology is nascently embedded within our industry and its deployment will only expand in the coming years. Thus, it is important to grapple with the issues it presents before it brings about unwelcome surprises. Rather than retrofitting controls, as was the case when cyber security concerns first emerged, boards should be attentive to ensuring that the deployment is well controlled and understood from the beginning.

In this respect, directors may wish to create an AI oversight framework. This framework will necessarily involve new topics and concerns. In addition, existing oversight functions may take on new dimensions to deal with oversight of AI applications.

Oversight Framework

At the outset, a fund board may wish to understand the adviser's approach to the use of AI and request periodic briefings at board or committee meetings. Topics might include:

1. Has the adviser mapped the areas within its organization where it is currently or could deploy AI applications and identified related gating items and codependences for further deployment?
2. Is the adviser applying a "sandbox" approach to potential applications?
3. Does the adviser have a strategy for the use of AI with respect to portfolio management, digital engagement processes and other applications?
4. Has the adviser assessed risks and threats associated with the use of AI?
5. Has the adviser developed a thoughtful governance and accountability program covering its AI applications and related risks and threats?
6. The more an AI system learns, the further it gets from its initial programming. Has the adviser built in robust testing before launch, a continuous testing program, and strong controls to ensure that outcomes continue to fall within expectations?

Enhancements To Existing Oversight Functions

Use of AI may impact familiar oversight functions. A fund board may seek additional information in connection with its existing oversight of the following matters:

1. *Cybersecurity*. Threat actors using AI may pose new and more complex threats. The ability of AI agents to mimic human communication and the low cost of scaling AI agents increase opportunities for fraud, phishing and other cyber threats. AI may also be used defensively.
2. *Outsourcing and vendor management*. Does the adviser understand the use and AI capabilities of

existing vendors? Fund advisers should also be identifying and vetting vendors that offer AI-based products. For example, law and accounting firms are increasingly relying on AI enhanced products and specialized AI products have been developed for multiple industries. Advisers should have a full understanding of where AI is being employed in their vendor ecosystem, how their data is being used to train the vendor's AI models, and related risks and opportunities.

3. *Concentration risk*. The asset management industry is already subject to risk from its concentration of key vendors. As Chair Gensler has pointed out, there may be overreliance "on one base level, what's called [the] generative AI level," with multiple fintech applications built on top of that level.⁴³ Failure at the generative AI level could then cause cascading failure. As an example, today there are multiple front-end brokerage apps, but close to 90 percent of the dollar volume of trading is executed by three wholesalers. Reliance on base-level technology is not always apparent.
4. *Supervision and systems controls*. Many fund advisers have initially chosen to ban or limit use of AI tools within their firms. How is the use of AI monitored within the adviser's operations? Has the adviser provided guidance or training to employees on the use of AI systems and assessed any confidentiality and privacy concerns? Does the adviser track which individuals at the adviser and which third party vendors have access to the firm's AI models and data inputs and outputs?
5. *Data privacy*. Collecting and using proprietary data or customer data for AI applications should be closely monitored for compliance with privacy laws. It also is possible that vendors are training their own AI on data gleaned from the adviser. How does the adviser protect its own data and that of shareholders?
6. *Disclosure*. The use of AI may require revised or enhanced risk disclosure.

New and Novel Issues

Some aspects of AI raise novel questions:

1. It has been suggested that flaws in the design or application of AI technology can create enterprise-level risks because a coding error or mistake in design can be rapidly repeated prior to detection. Fund boards should seek to understand how these risks are mitigated.
2. Ensuring that the technology is transparent and explainable. As noted above, this has been an area of regulatory concern and is emphasized in the proposed AI Conflicts of Interest Rule. It is also important that portfolio managers and those charged with oversight and control, not just technologists, understand how applications function.
3. Avoiding biases and discriminatory outputs, especially in employment and interactions with clients. Where digital engagement practices are utilized, this raises particular concerns.
4. The deployment of AI raises both ethical and commercial issues for workforce management. Fund boards may wish to understand the fund adviser's strategy with respect to whether the use of AI will enhance employee skills, productivity and career opportunities or result in job displacements.

Model Risk

Use of AI can create model risk. Directors should seek to understand the governance and controls framework covering the development and use of AI based models. Elements of "model governance" can include:

1. Ensuring that algorithms operate as intended. The initial design should incorporate compliance with all relevant laws and regulations. The design should be subject to regular testing of outcomes. Embedded assumption should be regularly refreshed.
2. Ensuring explainability of an algorithm's core operations, an understanding of the data sets the model was trained on, and the potential for data drift over time.
3. Understanding and disclosing material limitations or risks associated with the use of an algorithm.
4. An oversight framework that draws on expertise across the enterprise. It is important to ensure that senior management, risk management personnel, compliance personnel and internal control have an understanding that is sufficient to recognize and mitigate relevant risks arising from use of the model.

Conclusion

As with all technologies, the widespread deployment of AI will likely come with both costs and benefits. Its use also will generate new regulations and compliance considerations. Understanding the basics of how it works, regulatory considerations, and the risks and opportunities it provides is increasingly important for directors to effectively discharge their watchdog role.

Ms. Moynihan is a partner at Perkins Coie LLP in Washington, DC. **Ms. Ganapathy** is senior counsel at Perkins Coie LLP in New York, NY. The authors would like to acknowledge Henry Little and Stephanie Flynn, Summer Associates at Perkins Coie, for their assistance in preparing this article.

NOTES

- ¹ OpenAI, "Introducing ChatGPT," OpenAI Blog (Nov. 30, 2022), <https://openai.com/blog/chatgpt>.
- ² Darrell M. West, "What is artificial intelligence?," *BROOKINGS* (Oct. 4, 2018), <https://www.brookings.edu/articles/what-is-artificial-intelligence/#:~:text=Turing%20was%20followed%20up%20a,are%20said%20to%20involve%20intelligence.%E2%80%9D>.

- ³ “NIST Releases Draft Plan for Federal Engagement in AI Standards Development,” *Nat’l Inst. Standards & Tech.*, (July 26, 2021), <https://www.nist.gov/news-events/news/2019/07/nist-releases-draft-plan-federal-engagement-ai-standards-development>.
- ⁴ “What is artificial intelligence (AI)?,” IBM (last visited Sept. 19, 2023), <https://www.ibm.com/topics/artificial-intelligence#:~:text=AI%20is%20simplest%20form%2C%20artificial,in%20conjunction%20with%20artificial%20intelligence>.
- ⁵ “How Does Chat GPT Work?,” *TechRound* (last visited Sept. 19, 2023), <https://techround.co.uk/guides/how-does-chat-gpt-actually-work/>.
- ⁶ Gary Gensler, Chair “Isaac Newton to AI,” Remarks before the National Press Club, U.S. Sec. & Exch. Comm’n (July 17, 2023).
- ⁷ “What is a neural network?,” IBM (last visited Sept. 19, 2023), <https://www.ibm.com/topics/neural-networks>.
- ⁸ *Id.*
- ⁹ Anne Geyer, “GPT-4: What You Need to Know and What’s Different from GPT-3 and ChatGPT,” *Ax-Semantics Blog* (March 13, 2023), <https://en.ax-semantics.com/blog/gpt-4-and-whats-different-from-gpt-3/>.
- ¹⁰ Jan Hatzius *et al.*, “Global Economics Analyst, The Potentially Large Effects of Artificial Intelligence on Economic Growth,” Goldman Sachs (March 26, 2023, 9:05 PM), <https://www.gspublishing.com/content/research/en/reports/2023/03/27/d64e052b-0f6e-45d7-967b-d7be35fabd16.html>.
- ¹¹ Tiago Bianchi, “Distribution of bot and human web traffic worldwide from 2014 to 2022,” *Statista* (July 17, 2023), <https://www.statista.com/statistics/1264226/human-and-bot-web-traffic-share/>.
- ¹² Justina Lee & Saijel Kishan, “Hedge Funds Are Deploying ChatGPT to Handle All the Grunt Work,” *Bloomberg* (May 31, 2023, 5:00 AM), <https://www.bloomberg.com/news/articles/2023-05-31/hedge-funds-are-deploying-chatgpt-to-handle-all-the-grunt-work#xj4y7vzkg>.
- ¹³ Renaissance Technologies LLC, Acad. Accelerator Encyc. (last visited Sept. 19, 2023), <https://academic-accelerator.com/encyclopedia/renaissance-technologies>.
- ¹⁴ Ryan W. Neal, “AI arrives on Wall Street,” *Investment News* (July 10, 2023), <https://www.investmentnews.com/ai-arrives-on-wall-street-239607>.
- ¹⁵ Artificial Intelligence ETF List, VettaFi (last visited Sept. 19, 2023), <https://etfdb.com/themes/artificial-intelligence-etfs/>.
- ¹⁶ “Investors Can Now Let AI Buy the Dip for Them Thanks to a New AI-Power ETF,” *Access Wire* (Jun. 14, 2023).
- ¹⁷ “About AIEQ,” *eftmg* (last visited Sept. 19, 2023), <https://etfmg.com/funds/aieq/>.
- ¹⁸ A Differentiated Approach to Navigating Market Downturns with Qraft’s AI Pilot, Qraft AI ETFs (last visited Sept. 19, 2023), <https://www.qraftaief.com/aidb>.
- ¹⁹ Nathan Reiff, “Jim Rogers Launches AI-Driven ETF,” *Investopedia* (June 21, 2018), <https://www.investopedia.com/news/jim-rogers-launches-aidriven-etf/>.
- ²⁰ James Manyika *et al.*, “What Do We Do About the Biases in AI?,” *Harv. Bus. Rev.* (Oct. 25, 2019), <https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai>.
- ²¹ Notice of Adoption of Final Rule, N.Y.C. Dep’t Consumer & Worker Prot. (Apr. 6, 2023), <https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf>.
- ²² Getty Images has sued Stability AI, Inc. (Stability) for both copyright and trademark infringement, alleging that Stability copied more than 12 million photographs from Getty Images’ collection. *Getty Images (US), Inc. v. Stability AI, Inc. et al.*, No. 1:2023cv00135 (D. Del. filed Feb. 3, 2023).
- ²³ *Id.*
- ²⁴ Class Action Complaint filed in Andersen *et al. v. Stability AI Ltd. et al.*, No. 3:23-cv-00201 (N.D. Cal. filed Jan 13, 2023).
- ²⁵ The US Copyright Office has declined to register a work that was created by AI. *See*, Letter from U.S. Copyright Rev. Bd. to Ryan Abbott, Esq. (Feb. 14, 2022), <https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf>.

- ²⁶ Federal Trade Commission (FTC) Civil Investigative Demand (CID) Schedule FTC File No. 232-3044, U.S. Fed. Trade Comm’n (last visited Sept. 19, 2023).
- ²⁷ “EU AI Act: first regulation on artificial intelligence,” *News Eur. Parl.* (June 14, 2023 14:06), [https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence;ArtificialIntelligenceAct,2021/0106\(COD\)Legis.ObservatoryEur.Parl.\(June14,2023\),https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747977&t=e&l=en#:text=Its%20aim%20is%20to%20promote,intelligence%20systems%20in%20the%20Union](https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence;ArtificialIntelligenceAct,2021/0106(COD)Legis.ObservatoryEur.Parl.(June14,2023),https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747977&t=e&l=en#:text=Its%20aim%20is%20to%20promote,intelligence%20systems%20in%20the%20Union).
- ²⁸ Blueprint for an AI Bill of Rights, White House Off. Sci. & Tech. Pol’y (last visited Sept. 19, 2023), <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.
- ²⁹ *Id.*
- ³⁰ *Id.*
- ³¹ Andrew Ross Sorkin *et al.*, “The S.E.C.’s Chief Is Worried About A.I.,” *N.Y. Times* (Aug. 7, 2023), <https://www.nytimes.com/2023/08/07/business/dealbook/sec-gensler-ai.html>.
- ³² See, Gary Gensler, Chair, Investor Protection in a Digital Age, Remarks Before the 2022 NASAA Spring Meeting & Public Policy Symposium, U.S. Sec. & Exch. Comm’n (May 17, 2022), https://www.sec.gov/news/speech/gensler-remarks-nasaa-spring-meeting-051722#_ftnref11.
- ³³ *Id.*
- ³⁴ John Divine, “How AI Could Spark the Next Financial Crisis,” *U.S. News* (June 30, 2023), <https://money.usnews.com/investing/articles/how-ai-could-spark-next-financial-crisis-gensler>.
- ³⁵ Davey Alba, “How Fake AI Photo of a Pentagon Blast Went Viral and Briefly Spooked Stocks,” *Bloomberg* (May 23, 2023), <https://www.bloomberg.com/news/articles/2023-05-22/fake-ai-photo-of-pentagon-blast-goes-viral-trips-stocks-briefly#xj4y7vzkg>.
- ³⁶ Stephen Sanford, “How to Build Accountability into Your AI,” *Harv. Bus. Rev.* (Aug. 11, 2021), <https://hbr.org/2021/08/how-to-build-accountability-into-your-ai>.
- ³⁷ *Supra*, n.6. See also, “What is explainable AI,” IBM (last visited Sept. 19, 2023), <https://www.ibm.com/topics/explainable-ai>.
- ³⁸ Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers 88 Fed. Reg. 53960 (Aug. 9, 2023), <https://www.govinfo.gov/content/pkg/FR-2023-08-09/pdf/2023-16377.pdf>.
- ³⁹ Covered technologies include analytical, technological, or computational function, algorithm, model, correlation matrix, or similar method or process that optimizes for, predicts, guides, forecasts, or directs investment-related behaviors or outcomes. This proposed definition is specifically designed to capture predictive data analytics (PDA) like technologies, such as AI, machine learning, or deep learning algorithms, neural networks, NLP, or large language models (including generative pre-trained transformers), as well as other technologies that make use of historical or real-time data, lookup tables, or correlation matrices, among others. Technologies that are designed to inform investors (website with current account balance or past performance) but do not guide or direct any investment-related action or a chatbot that employs technology to assist investors with basic customer service support (password resets or disputing fraud) would not qualify as covered technology. *Id.* at 53972.
- ⁴⁰ Press Release, “SEC Proposes New Requirements to Address Risks to Investors from Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers,” 2023-140 U.S. Sec. & Exch. Comm’n (July 26, 2023), <https://www.sec.gov/news/press-release/2023-140>.
- ⁴¹ *Supra* n.38 at 53990.
- ⁴² *Id.* at 53980.
- ⁴³ *Supra* n.34.

Copyright © 2023 CCH Incorporated. All Rights Reserved.
Reprinted from *The Investment Lawyer*, November 2023, Volume 30, Number 11,
pages 11–20, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com

