FOLEY

FOLEY & LARDNER LLP

The Fast Follower's Guide to Recent AI Law

FALL 2024

FOLEY.COM

FOLEY & LARDNER LLP

FOREWARD

As investors, entrepreneurs, and engineers supercharge the development of artificial intelligence (AI) to the tune of US$184 billion in 2024, this new era will create both winners and losers. But avoiding the bleeding edge of technology is no easy task, especially where innovation outpaces regulation.

Welcome to *The Fast Follower's Guide to Recent AI Law*, a curated selection of the most important developments across the legal sphere. In each piece our team explores the risks and opportunities introduced by trends such as AI washing, algorithmic recruiting, AI-assisted inventorship, and agentic systems. Whether you are a legal professional, an AI enthusiast, or simply curious about the future of technology, this eBook aims to share the knowledge and insights needed to thrive in the AI frontier.

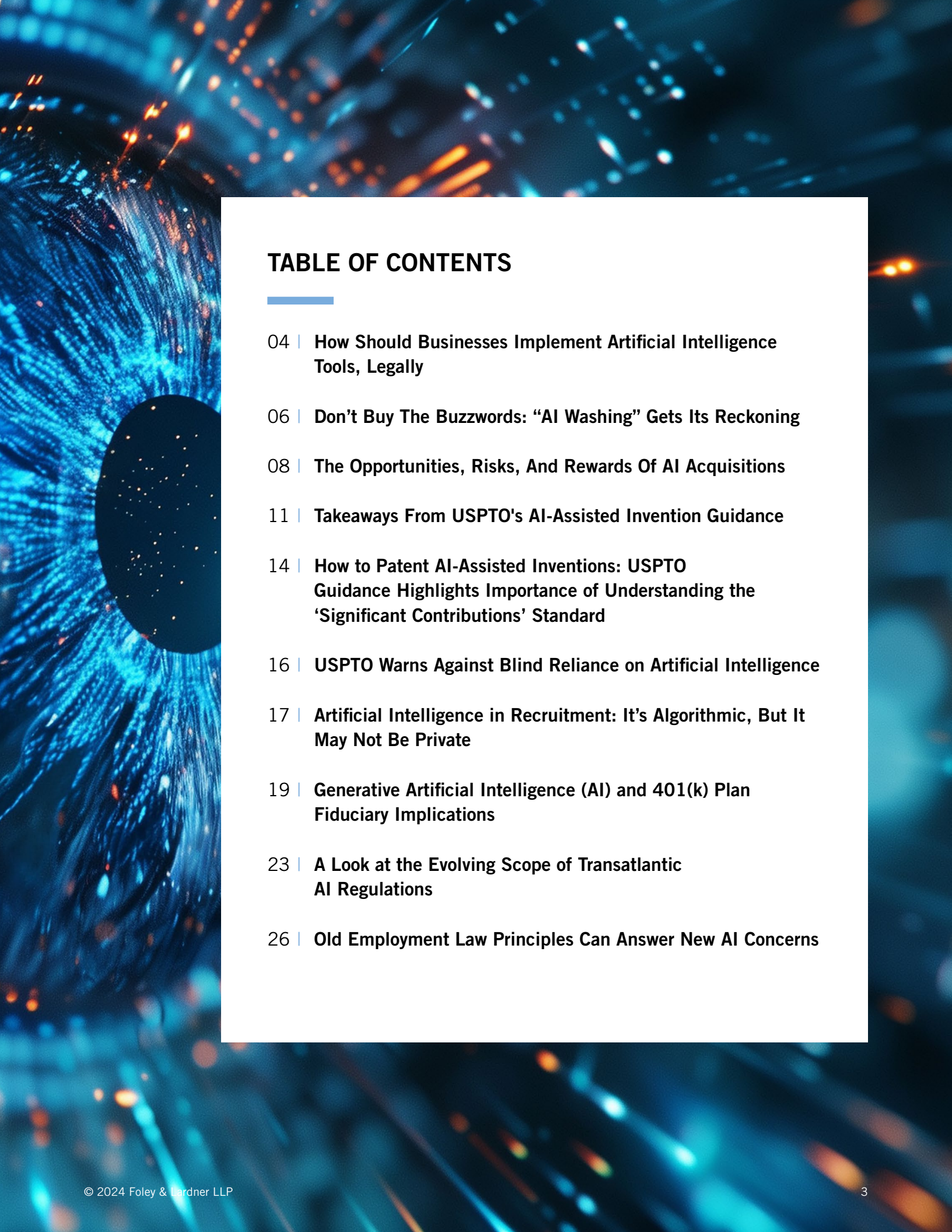


TABLE OF CONTENTS

How Should Businesses Implement Artificial Intelligence Tools, Legally

Published June 2024 by Foley & Lardner LLP

AUTHORS

Natasha Allen | nallen@foley.com

Louis Lehot | llehot@foley.com

Business leaders, from CEOs to CIOs to project managers, are rapidly adopting generative artificial intelligence (AI) tools to transform their organizations, harnessing the technology to drive efficiency, streamline processes, and enhance operational capability.

A KPMG survey revealed that nearly 65% of U.S. executives "believe generative AI will have a high or extremely high impact on their organization in the next three to five years, far above every other emerging technology." However, many admit they currently lack the necessary technology, talent, and governance to implement AI effectively. For example, many companies do not have a formal AI internal usage policy. These leaders are now investing considerable effort into understanding AI and strategizing its integration.

How are Corporate Leaders Leveraging AI Technologies Effectively?

Beyond automating repetitive tasks like customer service chatbots and robotic process automation (RPA) for administrative tasks, AI enhances critical decision-making by providing deeper insights into data. This includes predicting market trends, analyzing consumer behavior, and optimizing supply chains and resource management.

Furthermore, AI drives innovation and accelerates product development, particularly in sectors such as pharmaceuticals, high-tech, and automotive manufacturing. AI can expedite the R&D process, refine product design, and reduce time-to-market. These industries benefit from AI precision and efficiency resulting in an increased competitive edge.

AI can personalize the customer experience and aid marketers by analyzing large data sets to uncover customer behavior patterns. AI models can also assist with forecasting sales trends and market demand, enabling more effective resources and personalized customer interactions.

Practical Considerations for AI Implementation

Corporate leaders should be thoughtful when implementing AI, with end principles in mind. For example, we recommend the implementation of traceability applications to ensure that corporate users are adhering to AI-specific provisions in contracts and that employees are adhering to AI policies. When reviewing third-party vendor contracts, some vendors have revised their contacts to adopt AI language and governance without even mentioning AI-specific terms. A common usage of generative AI is to generate source code for common algorithms based on open-source libraries. Corporate leaders should ensure that employees are not using these databases to create critical IP that will lack authorship or IP rights.

What are Some of the Legal Issues Leadership Should Understand?

AI regulations are evolving and vary globally. States like California are developing AI legislation, and the EU has already enacted regulations. The United States lacks comprehensive legislation at the federal level, while state legislation is proliferating with varied outcomes. One legal area that has been much discussed is the issue of bias and discrimination, especially in the context of tools used by corporate HR departments. Many of the new laws being proposed, including one that just passed the Colorado legislature, have specific new requirements to deter potential bias and discrimination.

Different industries, such as health care organizations, higher education, and financial institutions are also subject to specific regulations that apply to the use of AI. With all this uncertainty and the patchwork of varied legislation, corporate leadership must do an in-depth analysis of where their business is situated, whether they are in a specifically regulated industry, and how to set up AI governance policies that make sense. Use your legal counsel to stay informed of pending legislation and how potential changes may have implications for your current and future business.

Corporate leaders also need to be aware of the changing legal landscape for privacy and security and the intersection with AI tools. For example, the data used in AI applications must be collected, used, and stored in compliance with all privacy regulations, such as GDPR and CCPA.

And, of course, there is the issue of intellectual property (IP) and ownership of the content that generative AI creates. Due to the ownership of the data inputs into generative AI engines, there are questions surrounding who owns the IP of the AI-generated outputs that have yet to be firmly decided, and company leaders would be advised to proceed with caution as they utilize the technology to produce content or even inventions. On a related note, the question of who is liable when an AI system causes harm or even fails is also in flux.

How can Corporate Leadership Move Forward With Implementation of AI Solutions?

Company leadership should collaborate closely with legal counsel to address these issues from the outset and create policies, plans, and procedures that comply with all applicable laws and regulations and mitigate risk. This also means staying on top of regulatory developments and updating policies as new laws come on board. Corporate leadership should also implement traceability solutions to ensure that employees adhere to these policies.

Employees should undergo meaningful training to understand the legal and ethical concerns surrounding AI, and regular audits should be conducted to identify any concerns over non-compliance, with a focus on deterring bias and discrimination. There is also a growing call for AI systems to be more transparent, with all stakeholders having a clear understanding of how the tools are making decisions. When companies implement more explainable AI technologies from the start, it can help to address this concern.

As with the implementation of any new technology in organizations, the benefits of AI come with risks, both known and unknown. The legal and regulatory landscape is evolving on a country-by-country, state-by-state basis. Every organization will need to assess whether and when to implement generative AI tools. Ultimately, organizations that fail to adopt new technologies will fail to compete on a quality and cost basis with their competitors, while those that implement it carelessly can experience detrimental effects. While we firmly believe the rewards will outweigh the risks, the assessment must be done, and the potential liabilities must be identified and ultimately mitigated. Working with experts, including legal counsel, developing a roadmap to implementation, adopting governance policies, and training your base of users and employees will all accelerate the quality and speed of adoption.

Don't Buy The Buzzwords: "AI Washing" Gets Its Reckoning

Published August 2024 by Foley & Lardner LLP

AUTHORS

Peter Fetzer | pfetzer@foley.com
Chanley Howell | chowell@foley.com
James Lundy | jglundy@foley.com
William McCaughey | wmccaughey@foley.com

Since the release of ChatGPT 3.5 in November 2022, public interest in artificial intelligence (AI) has surged in a classic example of a hype cycle. As with past technological breakthroughs, companies may be tempted to overstate their AI capabilities to draw investor attention.

But that may be coming to a swift end as the U.S. Securities and Exchange Commission (SEC) has begun paying close attention to this "AI Washing" trend and warning organizations against overstatement.[1]

What is AI Washing?

"AI Washing" is the intentional overstating of a product or service's AI capabilities to make such product or service appear more innovative or intelligent than it actually is, and thus "artificially" inflating sales or engagement. The phrase stems from "greenwashing" (which itself came from "whitewashing"), a term frequently used to describe companies, products, or services that exaggerate their efforts to reduce environmental impact for the sake of appealing to environmentally conscious consumers.

Regulators have been warning about the risks of AI Washing for some time. SEC Chair Gary Gensler, while speaking at an AI conference in December 2023, cautioned: "Don't do it…. One shouldn't greenwash, and one shouldn't AI wash. I don't know how else to say it." Reiterating those sentiments in prepared remarks at Yale Law School in February 2024, Gensler again cautioned companies against overstating their AI capabilities: "If a company is raising money from the public, though, it needs to be truthful about its use of AI and associated risk…. As AI disclosures by SEC registrants increase, the basics of good securities lawyering still apply. Claims about prospects should have a reasonable basis, and investors should be told that basis."

More recently, on April 15, 2024, Gurbir Grewal, Director of the SEC's Division of Enforcement, warned:

> If you are rushing to make claims about using AI in your investment processes to capitalize on growing investor interest, stop. Take a step back, and ask yourselves: do these representations accurately reflect what we are doing or are they simply aspirational? If it's the latter, your actions may constitute the type of "AI-washing" that violates the federal securities laws.

Yet, the impact of AI on our lives will continue to expand, and how AI is disclosed and discussed by companies and firms will continue to evolve in tandem with the risks associated with such disclosures. As Mark Zuckerberg posited during Meta's July 2024 earnings call, AI is going to affect almost every company's' products in some way; specifying that "this is why there are all the jokes about how all the tech CEOs get on these earnings calls and just talk about AI the whole time." This remark highlights the pressure that CEOs and companies face to hop on and keep up with the AI bandwagon.

Recent SEC Enforcement Actions

On March 18, 2024, the SEC announced its first ever settled charges against two investment advisers, Delphia and Global Predictions, for violating antifraud provisions of the Investment Advisors Act of 1940 through purported misrepresentations about their use of AI. Both companies claimed that they utilized certain AI technologies to attract investors, but did not actually use those AI capabilities.

Delphia publicly claimed that it used AI and machine learning to analyze client data to inform investment decisions, purporting that it "put[s] collective data to work to make [its] artificial intelligence smarter so it can predict which companies and trends are about to make it big and invest in them before everyone else." According to the SEC, Delphia's claims were false and misleading because Delphia did not have the AI capabilities it publicly represented.

Similarly, the SEC alleged that Global Predictions made false and misleading statements about its AI expertise as the "first regulated AI financial advisor" and its technologies that incorporated "[e]xpert AI-driven forecasts."

Delphia and Global Predictions both settled violations of Section 206(2) of the Advisers Act for their false and misleading statements. Both companies were also found to have violated the Marketing Rule, which makes it unlawful for registered investment advisers to produce advertisements that include any untrue statement of material fact. Delphia paid a civil penalty of US$225,000 and Global Predictions paid a civil penalty of US$175,000.

More recently, on June 11, 2024, the SEC announced litigated charges against the CEO and founder of a now-shuttered AI recruitment startup for alleged violations of the antifraud provisions of the Securities Act of 1933 and Securities Exchange Act of 1934. In its complaint, the SEC alleged that the CEO "engaged in old school fraud using new school buzzwords like "artificial intelligence" and "automation." The SEC further alleged that the CEO defrauded investors of at least US$21 million by making misleading statements about the quantity and quality of the company's customers, the number of candidates in its platform, and the company's revenue.

Director Grewal concluded his remarks in the press release with this admonition, "As more and more people seek out AI-related investment opportunities, we will continue to police the markets against AI-washing and the type of misconduct alleged in today's complaint. But at the same time, it is critical for investors to beware of companies exploiting the fanfare around artificial intelligence to raise funds."

Key Takeaways

As evidenced by these enforcement actions, the SEC is taking AI Washing very seriously and companies should be diligent and honest to ensure that they do not engage in this practice – either intentionally or inadvertently. To ensure compliance with the SEC's protocols, companies should consider the following:

- Fully and accurately disclose your AI usage. AI capabilities vary, so avoid using boilerplate language that is either overly vague or broad. Also avoid using vague or exaggerated claims and hypothetical examples to describe what your AI model is capable of doing.
- Be specific about the nature and extent of your AI technologies, the role AI plays in your business operations, and any potential risks or limitations associated with AI.
- Understand how your key service providers employ and use AI, as that will likely be the focus of future SEC oversight rules.
- Provide details about the company's AI implementations, including which processes, or products it impacts, the extent of its deployment, and any measurable outcomes.
- Establish and implement an AI governance framework to provide "scaffolding" for AI initiatives and ensure they align with the company's goals and ethical standards.
- Provide training for company marketing teams to ensure that technologies are properly labeled as "AI." Many technologies and algorithms do not actually qualify as AI but may be easily mistaken for it, so being aware of this before creating marketing materials will be crucial to avoid inadvertent AI Washing.
- Require that all public statements or advertising produced by the company regarding AI technologies be reviewed by the company's legal team to ensure the accuracy of such statements.
- Monitor the company's use and evolution of AI technologies, as well as external public statements regarding the company's use of AI technology and correct any misstatements or inaccuracies that may arise.
- Regularly update shareholders and other stakeholders on the progress, changes, and improvements in AI initiatives.

Special thanks to Natalie Smith, a summer associate in Foley's New York office, for her contributions to this article.

Endnotes

1 In addition to the risks of SEC enforcement, companies also face the threat of private securities class actions. Cornerstone Research found an uptick in securities class actions with allegations of AI-related deceptions. According to Cornerstone, investors filed six AI-related class actions between January and June of 2024, compared to six such actions in all of 2023.

The Opportunities, Risks, And Rewards Of AI Acquisitions

AUTHORS

Louis Lehot | llehot@foley.com
Natasha Allen | nallen@foley.com
David Kantaros | dkantaros@foley.com

Published May 2024 by Foley & Lardner LLP

This article was originally published in Law360 on May 20, 2024, and is republished here with permission.

Amid a period of recalibration, the artificial intelligence industry is experiencing a transformational phase.

According to a recent report from Stanford's Institute for Human-Centered Artificial Intelligence that closely monitors AI trends, there's been a notable adjustment in global investment patterns within the sector.

Despite a decline in overall AI private investment last year, funding for generative AI surged from 2022 to reach US$25.2 billion, and notable companies in the generative AI space, including OpenAI, Anthropic, and Mistral, reported substantial fundraising rounds.

AI ventures continue to attract significant investment, like Anthropic's recent multibillion-dollar investment from Amazon, and Apple has already started the year off with the acquisition of DarwinAI, a company working to make AI systems smaller and more efficient.

The potential of AI technologies is immense, with the global market projected to reach US$407 billion by 2027. This translates to an implied compound annual growth rate of 36.2% during the forecast period of 2022 to 2027. For buyers that are listening for the sound of opportunity knocking, here it is.

With AI acquisitions becoming an increasing area of focus for investors and technology buyers, this article will hone in on specific areas to focus on when structuring and executing a transaction with a company that has an AI-centric business model.

From target identification to due diligence to navigating regulatory frameworks, the journey of acquiring an AI company is better spent after careful preparation and strategic foresight.

Target Identification

As the cost of programming AI-powered algorithms and large language models comes down, buyers will look beyond pure engineering talent of the target team and seek to ensure that the target is acquiring unique and proprietary datasets.

It's no longer just about the algorithms and large language models, it's about having access to proprietary data that no one else can get, and the ability to use the data in the AI system in the manner desired. Sellers looking to position themselves for acquisition should highlight, expand and protect their access to proprietary data as much as engineering talent.

Due Diligence Concerns

Conventional due diligence practices in the tech industry often focus on tangible assets like proprietary software and hardware.

However, for AI companies, the real value lies in intangible assets.

Layered, multifunction algorithms where there are not likely to be patents, large language models that are unprotected by copyrights, and increasingly, the exclusive access to proprietary datasets that together produce valuable answers, will drive monetization.

And so it goes to reason that buyers need to conduct technical and legal due diligence to capture a wider range of the target's technology functionality. From

the legal and compliance side, buyers will need to understand where the target operates and from where can users access the product in order to determine the breadth and scope of applicable laws.

Similarly, buyers will want to ensure that data privacy rules are not violated, that cybersecurity is intact, and that copyrights are licensed or excluded. Buyers will also need to confirm the genealogy of the data, from its origin to the assignment to the buyer, and will want to establish that seller is transferring to buyer contractual rights to use the data for the buyer's intended purpose.

From a technology side, this means examining whether the AI solution is authentic, robust, scalable and aligned with business objectives. With thorough technical due diligence, investors can avoid exposure to "fake AI," or misrepresented solutions lacking genuine capabilities, potentially leading to substantial financial losses.

Key questions to address during the process include algorithms and models, purchase agreements, data privacy and security measures, and ensuring compliance with relevant regulations such as the General Data Protection Regulation or the California Consumer Privacy Act.

Additionally, look for industry-specific or geographical regulatory concerns, and consider how regulatory changes could affect the company's operations and future growth.

Special Considerations for Purchase Agreements

In crafting a purchase agreement for a company with an AI-centric business model, it's important to recognize the distinctive nature of AI systems. While conventional agreements cover typical risks associated with intellectual property or software, the unique attributes of AI demand special attention.

Buyers want assurances and guarantees from sellers to mitigate specific risks linked to the target company's business. However, standard provisions may not adequately address the complexities of AI, and lawyers must assess the AI company's risk profile thoroughly, considering its potential for high-risk outcomes.

Addressing these concerns requires tailored provisions in the purchase agreement. Considerations include representations and warranties regarding AI assets, encompassing ownership and noninfringement, not to mention compliance with data privacy rules and cybersecurity integrity and maintenance. Sellers must disclose any known risks or limitations associated with the AI technologies being transferred.

To manage risks effectively, buyers often seek indemnities for breaches of these representations and warranties. Additionally, holdbacks and escrow arrangements can be utilized to ensure sellers meet their obligations and address potential post-closing liabilities. Increasingly, third-party insurance carriers are underwriting these risks in the course of transactions.

Any combination of these measures can streamline the transaction process and promote clarity for the parties involved.

Navigating Regulatory Frameworks

As the regulatory landscape surrounding AI is nascent, governments and regulatory bodies worldwide are dealing with issues such as data privacy, algorithmic bias and ethical considerations. This becomes important for counsel involved in AI acquisitions, as they must stay abreast of potential changes and ensure compliance with relevant laws and regulations, especially those that are not yet in force or were never contemplated when the business was created.

According to the Stanford University AI Index Report, the number of AI-related regulations in the U.S. has risen significantly over the last five years.

In 2023, there were 25 AI-related regulations, up from just one in 2016. Last year alone, the number of AI-related regulations grew by 56.3%. In 2023, the count of U.S. regulatory bodies crafting AI regulations climbed to 21, up from 17 in 2022, signaling an expanding interest in AI governance across a broader spectrum of American regulatory entities.

Among the newcomers to implement AI-related regulations for the first time in 2023 are the U.S. Department of Transportation, the U.S. Department of Energy, and the Occupational Safety and Health Administration.

Adherence to data privacy regulations such as the General Data Protection Regulation, the California Consumer Privacy Act, and the Health Insurance Portability and Accountability Act is especially important for businesses that collect, process, and

create data outputs containing or based on datasets containing sensitive personal information.

Acquisitions of AI companies are facing special scrutiny from antitrust and competition regulators around the world, who are concerned with not only monopolistic practices and anti-competitive behavior, but also about the effect of AI on jobs.

Effect on AI Startups From Acquisition

Major Big Tech firms significantly shape the trajectory of AI startups.

The outcomes of AI acquisitions hinge on various factors, such as the preservation or erosion of autonomy, cultural integration, and the fostering of innovation within the acquired entity. For instance, Google's acquisition of DeepMind stands as a model of success, as DeepMind has retained its autonomy under Google's umbrella, fostering continued innovation.

Conversely, Apple's assimilation of Siri, one of Steve Jobs' final major creations, saw it lose autonomy as it became Apple's voice assistant.

Cultural clashes during integration can lead to the departure of key personnel, yet some acquisitions manage to maintain cultural harmony. The spectrum of outcomes and effects from acquiring AI startups encompasses triumphs and hurdles for the involved parties.

While acquiring an AI company offers substantial prospects for growth and innovation, the risk profile for AI-centric business models is so different from acquisitions of other technology businesses that a new approach is required.

With a retargeted due diligence investigation, tailored purchase agreement, and adherence to regulatory mandates, buyers can optimize the benefits of acquiring an AI company and avoid the many hidden pitfalls.

Takeaways From USPTO's AI-Assisted Invention Guidance

AUTHORS

James De Vellis | jdevellis@foley.com
Austin Kim | akim@foley.com
Abdullah Akhtar | aakhtar@foley.com

Published March 2024 by Foley & Lardner LLP

This article was originally published in Law360 on March 8, 2024. Republished with permission.

Pursuant to efforts by the federal government to develop artificial intelligence in a safe, secure, and trustworthy manner, the U.S. Patent, and Trademark Office issued inventorship guidance for inventions developed with assistance of AI in February.

The guidance clarifies how inventorship is to be determined for the purposes of a patent when AI is involved in the innovation process. It also shows the USPTO's commitment to adapting examination practices to keep pace with the fast-evolving technological field.

Background

The issuance of the guidance is driven in part from recent attempts to name an AI agent as an inventor of a patent.

Starting in 2019, the Artificial Intelligence Project attempted to obtain a patent listing an AI agent named "Device for Autonomous Bootstrapping of Unified Sentience" as the inventor in a number of jurisdictions, including the U.S.

The USPTO rejected the patent application, declaring that an inventor must be a natural human being.

Stephen Thaler — in his role as representative for the Artificial Intelligence Project — in turn fought the ruling through the U.S. District Court for the Eastern District of Virginia and the U.S. Court of Appeals for the Federal Circuit, both of which upheld the USPTO's decision of refusal.

At each stage of this ordeal, Thaler had argued that the AI agent should be recognized as an inventor to promote innovation and that the Patent Act does not preclude the listing of an AI agent as an inventor.

Neither the USPTO nor the courts were persuaded by these arguments. The Federal Circuit in particular pointed to a number of sections from the Patent Act emphasizing that the inventor should be a natural person.

Affirming the district court's decision, the Federal Circuit found that the Patent Act specifically noted that the statute consistently uses the term "individual" when referring to inventors and co-inventors in Title 35 of the U.S. Code, Sections 100(f), 100(g) and 115.

The Federal Circuit, however, also left open the door on "whether inventions made by human beings with the assistance of AI are eligible for patent protection."

USPTO Guidance

In line with these rulings, the USPTO reaffirmed that AI entities cannot be named as inventors.

Drawing from past jurisprudence on joint inventorship, the guidance specifies that an individual associated with an AI-assisted invention can be deemed an inventor when the individual has made a significant contribution to the claimed invention.

The guidance relies on the Pannu factors — a three-part test articulated in Pannu v. Iolab Corp. in the Federal Circuit in 1998 — in determining what constitutes a significant contribution:

1. Contribute in some significant manner to the conception or reduction to practice of the invention.

2. Make a contribution to the claimed invention that is not insignificant in quality, when that contribution is measured against the dimension of the full invention.

3. Do more than merely explain to the real inventors well-known concepts and/or the current state of the art. The guidance applies the Pannu factors to the context of AI-assisted inventions and provides a list of principles to help applicants and examiners determine whether a natural person using an AI system should be listed as an inventor for the purposes of a patent based on the person's contributions.

Under the guidance, a natural person can be listed as an inventor even if the natural person relied on or used an AI system when the person's contribution is deemed significant.

Second, a person who merely presents a problem to an AI system and identifies the output from the AI system cannot be considered an inventor; on the other hand, if the person constructed the input prompt to the AI system in a particular way to elicit a particular solution, the person's contribution could rise to the level of significance for inventorship.

Third, a person who merely reduces an invention to practice alone is not a contribution that rises to the level of inventorship. For example, someone who appreciates the output of an AI system especially when the "properties and utilities are apparent to those of ordinary skill," is not necessarily an inventor.

Fourth, a person who designs an essential building block, such as building or training the AI system in view of a specific problem to elicit a particular solution, can be considered to have provided a significant contribution.

Fifth, an individual who maintains intellectual domination over the AI system does not — on its own — make the individual an inventor of any of the inventions created in conjunction with the AI system.

The guidance notes that if no natural person has made any significant contribution to the claimed invention, then no inventors can be named, and the application should be rejected on Title 35 of the U.S. Code, Sections 101, and 115, grounds.

Examples Provided by USPTO

In furtherance of the guidance, the USPTO also provided two examples illustrating how inventorship should be determined for claims related to AI-assisted inventions.

The first example provides a narration of how a transaxle for a toy remote control car was created. Here, two natural persons rely on an AI system to create a preliminary design for a transaxle and appreciate that the output design could be used in the remote control car.

This example presents five scenarios, each with varying levels of human involvement in the conception of the transaxle design:

1. Natural persons take output from an AI system without any alteration.

2. Natural persons make minimal alterations to the output of the AI system, while reducing the transaxle to practice.

3. Natural persons perform experiments on the AI output to create a modified design.

4. Natural persons use an AI system to make minor alterations to a new design that they came up with.

5. The owner of an AI system attempts to patent a transaxle design.

In line with the USPTO's own guidance, the example explains that the individuals under the first and second scenarios cannot be considered proper inventors under the first through third guiding principles laid out above, because they did not make any significant inventive contribution other than appreciating that the design would work and reducing the design to practice.

On the other hand, the example lays out that the individuals under the third and fourth scenarios can be considered proper inventors for the purposes of a patent.

In the third scenario, the example highlights that these natural persons made significant contributions by conducting experiments to see how to modify the original design and that these modifications were integral to the claimed invention.

In the fourth scenario, the example notes that the use of the AI system to modify a new design does not negate the individuals' contributions as inventors.

As for the fifth scenario, the example notes that the owner of the AI system, which the two individuals used, cannot be considered an inventor for the patent only on the ground of ownership.

This example puts forth a concrete, real-world example of what to consider when deciding whether to name an individual as an inventor on a patent.

Conclusion

The new USPTO guidance regarding AI and inventorship is set to shake things up for patent practitioners.

The patent practitioners will need to get up to speed on the specifics of the guidance and how it applies to their clients' inventions.

This includes advising clients on how to document the inventive process in a way that meets the USPTO's new requirements. For example, merely presenting a problem to an AI and acknowledging its initial output will not qualify one for inventorship.

Instead, inventorship will require conducting experiments, modifying the AI's output, or providing essential building blocks for the claimed invention, among other actions, to make a significant contribution.

The USPTO guidance also emphasizes the importance of the duty of disclosure and the duty of reasonable inquiry. In this regard, patent practitioners will need to adjust their practices to accommodate the new guidance.

For example, under the duty of reasonable inquiry, patent practitioners should take keen notes on the facts and circumstances surrounding the process leading up to the conception of an invention, especially when an AI system is involved with a portion of this process.

Practitioners should be aware that:

- The mere use of an AI system does not negate an individual's inventive contribution.
- The presentation of the problem to the AI system and recognition of the use of the output from the AI system does not on its own constitute significant contribution.
- Reduction of the invention to practice is not sufficient for inventorship.
- The development of an essential block for the claim invention could constitute significant contribution.
- Ownership or intellectual dominion over an AI system on its own does not confer the person the title of inventor.

The new guidance should be seen as a positive step to boosting the burgeoning, nascent field of AI, with a global market for AI expected to reach a staggering US$1.8 trillion by 2030.

The guidance regarding the use of AI systems to assist in providing technical solutions to technical problems aligns with the long-standing principle that inventors must be natural people.

The principles laid out in the guidance are not a deviation from legal precedent, but rather a clarification applied to the rapidly growing field of AI-assisted innovation. The USPTO's guidance brings clarity to the issue of inventorship in the age of AI-assisted inventions.

This clarity should help ensure patents are granted to the rightful inventors, those who make significant contributions to the inventive process.

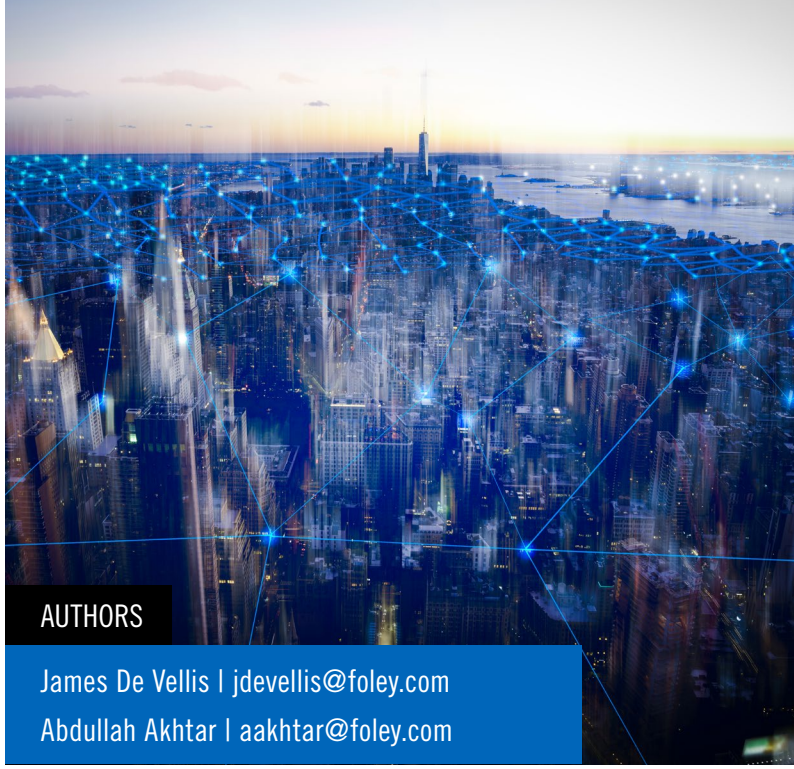
Navigating this terrain, however, comes with its own hurdles. Figuring out what exactly counts as a significant contribution when AI is part of the invention process is not always clear-cut.

For example, the new guidance could spark controversies regarding who rightfully deserves credit for an invention, particularly in cases where AI systems play a pivotal role.

While there are some uncertainties, the immediate risk of prosecution for failing to meet the new inventorship standards appears low. The extent to which examiners will scrutinize AI involvement in inventions remains to be seen.

All in all, while AI will significantly accelerate the pace of innovation, benefiting everyone, it is human ingenuity, and creativity that will continue to drive invention and patenting activity for the foreseeable future.

How to Patent AI-Assisted Inventions: USPTO Guidance Highlights Importance of Understanding the 'Significant Contributions' Standard



AUTHORS

James De Vellis | jdevellis@foley.com

Abdullah Akhtar | aakhtar@foley.com

Published July 2024 by Foley & Lardner LLP

The rapid rise of artificial intelligence (AI) has opened up exciting possibilities for innovation, but also uncertainty around who gets credit for inventions developed with the assistance of an AI system. At its core, there lies a fundamental question: who can be named as an inventor on a patent for an AI-assisted invention? In 2022, the U.S. Court of Appeals for the Federal Circuit highlighted this uncertainty by upholding the USPTO's rejection of patent applications that named an AI system, DABUS, as an inventor.

To address this, the U.S. Patent and Trademark Office (USPTO) issued guidance this February clarifying that AI entities, by themselves, cannot be named as inventors. However, the USPTO recognizes that humans working alongside AI can make significant contributions, and these contributions can qualify for inventorship.

The key concept here is the "significant contribution" standard, which has been used for the past 26 years after it was set forth in *Pannu v. Iolab Corp.*, 155 F.3d 1344, 1351 (Fed. Cir. 1998). Despite massive technological advances in the decades since this decision, the *Pannu* standard still applies to inventorship analyses, including those involving AI. Thus, the purpose of the USPTO's guidance is to inform the application of the *Pannu* inventorship standard to present-day scenarios where an AI system may be involved in the inventive process.

What Level of Human Involvement Amounts to a "Significant Contribution"?

For AI-assisted inventions to be patentable, the level of human involvement during the inventive process must satisfy the "significant contribution" standard. In what follows, different levels of human involvement will be explored to understand the practical implications of the standard and pave the way for successfully defending patent applications for AI-assisted inventions.

I. Contributions to the Claimed Inventions

Low involvement (not a significant contribution): In the realm of AI-assisted inventions, minimal human involvement translates to a lack of significant contribution for inventorship purposes. Simply feeding a general problem to an AI system and accepting its output verbatim would not qualify. Likewise, simply implementing the AI's output into practice, such as building a device or running a test based on the AI's recommendation, without any modifications would fall short of the inventive step required.

Medium involvement (potentially a significant contribution): The line blurs when human decisions come into play during the reduction to practice. If these decisions go beyond the AI's suggestions and address specific challenges, they have the potential to be considered significant contributions.

For example, the individual can go beyond the AI's suggestions by modifying the design of an invention. This may involve selecting a specific material to address a weakness in the AI's output or making strategic changes to improve functionality.

The level of contribution depends on the specifics and often hinges on whether the decision is

something a person of ordinary skill in the art would make. For example, selecting a common material for mechanical housing may not amount to a significant contribution. However, if the individual identifies a technical issue with the housing and strategically selects a different material to address the problem, that could be inventive.

High involvement (a significant contribution): The key here is recognizing a technical issue and making targeted modifications to solve it. Beyond material selection, other types of modifications could also demonstrate significant contributions. This could include recognizing deficiencies in the AI-generated design and modifying it through experimentation, altering the component's shape, relocating parts within it, or developing entirely new parts.

The principle of significant contribution through modification extends to other technical fields. For example, in developing a chemical compound, an individual can use an AI system to generate candidate compounds. If the individual then synthesizes, tests, and – importantly – refines these compounds to arrive at the final product, that hands-on approach would likely demonstrate a significant contribution and therefore patentable human inventorship. Moreover, modifying the structures of the generated compounds during experimentation could be considered a significant contribution.

II. Contributions to the Development of the AI System Used During the Inventive Process

In addition to contributions during invention, there is typically at least one individual who develops, trains, or supervises the AI system used. The level of contribution to the AI's development can also influence inventorship.

Low involvement (not a significant contribution): Simply supervising or maintaining an AI system during the inventive process would not constitute a significant contribution. Developing a general-purpose AI system without a specific problem in mind would not qualify either.

Medium involvement (potentially a significant contribution): There are instances where the individual who developed the AI could be listed as an inventor. For this to happen, the development and training of the AI system must be in response to, and specifically tailored to, solving a well-defined technical problem. The specific nature of the problem being addressed plays a role here — a more general problem definition could create a gray area for inventorship.

High involvement (a significant contribution): Consider the example of developing a new chemical compound. If the individual faces challenges during experimentation and, in response, creates and trains an AI system specifically designed to optimize compound structures based on a set of desired properties, such development and training could be considered significant contributions to the invention.

Conclusion: Documentation and Policies are Key

The "significant contribution" standard is paramount for practitioners and applicants navigating AI-assisted inventorship. To minimize inventorship challenges, detailed documentation is important. This documentation should capture the methodology, modifications, and experimentation undertaken by individuals throughout the inventive process, especially when AI systems are involved. Remember: the focus on inventive steps that address the specific technical challenge, not just general involvement, is what ultimately leads to a successful claim of inventorship.

While failure to follow these guidelines could result in the denial of patent rights, compliance allows innovators to leverage AI to solve a technical problem while maintaining space for a significant human contribution. This enables the procurement of valuable patents, with a proper human inventor, that are built to survive an inventorship challenge and can then be used to achieve specific business objectives. Accordingly, technology companies would be well suited to put policies in place that align with the USPTO guidelines in order to achieve appropriate protection for their AI-assisted innovations.

Special thanks to Bella Diehl, a summer associate in Foley's Boston office, for her contributions to this article.

USPTO Warns Against Blind Reliance on Artificial Intelligence

AUTHOR

Randy Pummill | rpummill@foley.com

Published February 2024 by Foley & Lardner LLP

U.S. Patent and Trademark Office (USPTO) Director Kathi Vidal released a memorandum on the subject of the use of artificial intelligence (AI) by parties during proceedings before the Trademark Trial and Appeal Board (TTAB) and the Patent Trial and Appeal Board (PTAB). In the memo, Director Vidal warns that parties are responsible for the content of their filings before the Boards, even when assisted by AI.

Concerns About AI Misuse

Director Vidal begins by recognizing that AI has already presented challenges for judges in other forums. While Chief Justice John Roberts has observed that AI "has great potential to dramatically increase access to key information for lawyers and non-lawyers alike," AI may also present false information as fact. For example, in a widely reported incident, in the Southern District of New York a lawyer turned in a brief including citations to cases that were made up or "hallucinated" by a popular AI tool. Last year, two attorneys were fined for their use of hallucinated cases in a brief. Director Vidal expresses concerns that misuses of AI will add delays and incur unnecessary costs on parties before the TTAB and PTAB.

Responsibility Lies on the Parties

Director Vidal notes that the USPTO has rules in place to prevent parties from engaging in misconduct. The USPTO Rules of Professional Conduct require that any signatory to a submission to either of the Boards certifies *inter alia* "that all statements made therein of the party's own knowledge are true, that any legal contentions are warranted by existing law or by a nonfrivolous argument for the extension…or reversal of existing law, and that factual contentions have evidentiary support." The memo further notes that it is not enough to assume any AI tools used to create a submission to the PTO are providing correct information. All signatories to a filing thus have a duty to ensure that the filing meets the criteria stated in the rules. Practitioners are also reminded that sanctions are available under the rules, from "[s]triking the offending paper" up to "[t]erminating the proceedings in the Office." Knowing and willful violations could result in criminal liability.

Takeaways

The recent memo from Director Vidal makes it clear that all parties and practitioners appearing before USPTO Boards have a duty to ensure that all information presented in their filings is factually accurate and that any arguments pursued are based on valid legal positions. Practitioners and parties should be aware of the limitations of AI tools and should not assume that the material generated by them is fit for submission in a legal proceeding. Before submitting a filing to a Board, parties and practitioners should take extra care to review any material generated with the assistance of AI tools to ensure that the AI-generated material is indeed accurate. Of particular concern should be citations to legal cases, which should be thoroughly checked to ensure that the cases really exist and stand for the stated legal principle — of course, this remains good practice even when AI-generative tools are not used for a given filing.

The USPTO recognizes that the use of AI tools to generate material in the legal industry is becoming increasingly common. While AI tools have the potential to be incredibly helpful, these tools must be used judiciously and with an understanding that the ultimate responsibility for a filing lies with the people appearing before the Boards.

Artificial Intelligence in Recruitment: It's Algorithmic, But It May Not Be Private

AUTHOR

Mark Neuberger | mneuberger@foley.com

Published August 2024 by Foley & Lardner LLP

The past few years have seen a sharp increase in the use of artificial intelligence (AI) across a variety of industries and workplaces. Many businesses have implemented AI to help streamline the recruitment and hiring process in the hopes of making hiring fairer and more efficient. While AI has not been completely successful with respect to eradicating bias across hiring practices as some had hoped, employers might not have thought about how AI manages their employee and applicant data. There are a number of data privacy and security issues that can arise as a result of AI recruitment tools if employers are not vigilant about making sure they are not running afoul of local data privacy laws.

The very nature of AI is that it "learns" by taking in and processing large amounts of data. This means it must collect and store a large amount of sensitive employee and candidate information. Thus, every time someone inputs data or information to a publicly accessible AI system, there is a risk confidential information will be shared. With the AI environment growing and changing so rapidly, employers are also left to make sense of a patchwork of data privacy laws that dictate how they are allowed to use and store this data. Some states have privacy laws that exempt employee data from regulatory requirements, such as the Virginia Consumer Data Protection Act (VCDPA), where states like California require that businesses provide information of their data-handling practices to candidates through the California Privacy Rights Act (CPRA). If the act now pending in congress known as the American Privacy Rights Act becomes law, it will pull together the patchwork of state laws by requiring employers to provide notice to applicants and employees that AI is being used as well as give them the opportunity to opt out. In the meantime, while this data is essential for recruitment and hiring purposes, employers need to be on the lookout both for security breaches as well as being compliant under applicable laws.

Navigating Privacy Concerns

Before implementing AI as a tool for candidate assessment, employers need to understand what kind of information it is going to collect. When using outside vendors, inquire what, if any, anti-bias and privacy safeguards are in place. For example, the Americans with Disabilities Act (ADA) generally prevents employers from inquiring about physical or mental disabilities and using that information as factors in hiring; if not careful, employers could find themselves at the end of a lawsuit because their AI software was collecting certain information from candidates and using that information to make decisions about whether or not to advance them. As such, employers must make sure that the AI tools they are using are only collecting essential data and make sure not to share any information with it that they would not otherwise want published to a third party.

As AI technology continues to rapidly evolve, companies would do well to avoid AI systems that collect and determine "proxy" variables for private or personal attributes for the sake of increased accuracy, even though there is no comprehensive guidance on it yet. Some AI software claim they have the ability to discern a candidates' sexual orientation through facial recognition or that it can scour a candidate's social media to infer their race or political affiliation. While many state and federal courts have not yet introduced

legislation for analyzing and using such information as it relates to advancing AI technology, employers should err on the side of caution to avoid being exposed to liability for discriminatory hiring practices.

The Need for Robust Data Protection

Companies should make sure to implement sophisticated data encryption to help safeguard sensitive information and prevent potential breaches that could put companies on the hook for identity theft or financial losses. AI-powered encryption solutions can be fused with traditional encryption models that can be useful for automatically identifying suspicious data access patterns and thereby tighten security in response. Data protection will also require human oversight to make sure that candidate and employee data is kept secure. Companies should develop and implement clear policies that explain who should routinely have access to employee and candidate data, health histories, and biometric data. This includes providing training on how to use these AI systems and performing routine audits to make sure the tools remain fair.

Takeaways

As with any technology, employers should take comprehensive steps to prevent the disclosure of employee and candidate data when using AI systems. This can involve discussing software options with vendors, limiting the data collected, developing clear policies on how AI should be used, training HR and recruitment teams on how to use these tools while remaining compliant, and making sure they have robust encryption and data protection safeguards. Finally, because the technology of AI is growing so rapidly, companies should remain vigilant for the inevitable legislation regarding privacy and data use and make sure they stay up to date with compliance requirements.

Special thanks to Meredith McDuffie, a summer associate in Foley's Chicago office, for her contributions to this article.

Generative Artificial Intelligence (AI) and 401(k) Plan Fiduciary Implications

AUTHORS

Michael Abbott | mabbott@foley.com
Aaron Tantleff | atantleff@foley.com
Cullen Werwie | cwerwie@foley.com

Published April 2024 by Foley & Lardner LLP

AI is emerging as a major transformative force across various industries, including finance and retirement planning. Like everyone else, fiduciaries are increasingly turning to AI-powered tools and algorithms to optimize investment strategies, enhance decision-making processes, and improve participant outcomes. However, integrating AI in 401(k) plan management has its challenges. While fiduciaries have a duty to act prudently and in the best interest of plan participants, what does that mean in the era of AI? To understand what that means, fiduciaries should consider conducting a formal evaluation of AI's impact on their 401k plan. This may include looking at the investment selection process, investment performance, the investment advisor/manager process, recordkeeper capabilities, the potential risks of using (or not using) AI, and its impact on service and the plan participants' overall experience. Based on the results of a formal evaluation, ongoing fiduciary oversight of AI may be warranted.

401(k) Plan Fiduciaries and the Investment Committee Process

Most 401(k) plans are structured to provide a core menu of investments with specific choices selected by plan participants. Many plans offer a qualified default investment alternative selected by fiduciaries. Typically, 401(k) fiduciaries are organized into an investment committee (the Committee) whose duties are spelled out in a detailed charter. The Committee generally establishes the investment option menu that plan participants can select from, and frequently uses an ERISA 3(21) investment advisor to assist this selection process. This advisor is a fiduciary under ERISA because their advice is given to the Committee for a fee. However, even when using a 3(21) advisor, the advisor's recommendations cannot simply be rubber-stamped because the Committee retains ultimate authority to determine investment options offered to plan participants. In addition, some 401(k) plans offer self-directed brokerage accounts (SDBAs), which provide hundreds, if not thousands, of potential investment choices. U.S. Department of Labor guidance regarding fiduciary obligations related to SBDAs is currently pending.

In some cases, the 401(k) plan sponsor, typically an employer, is not comfortable reviewing or making fiduciary decisions and instead appoints an ERISA 3(38) investment manager, who actually creates and implements the investment menu available to plan participants.

AI's Impact on Retirement Plans and 401(k) Fiduciaries

Blackrock announced "The AI revolution in retirement" because "it can be used to extract early insights on economic activities across regions, which can be used to inform macro (e.g., regional) and micro (e.g., company level) tilts in portfolios." Blackrock is not an anomaly — AI is gaining traction in the retirement plan, investment, and financial services industries. Specifically, AI is used to:

- Track positive and negative words in documents, transcripts, and earnings calls;
- Personalize messages to plan participants and prospective customers (Vanguard's use of Persado);

- Assist financial advisors through the use of AI (Morgan Stanley's use of OpenAI GPT-4);
- Automate investing with digital robo-advisors (Charles Schwab's Intelligent Portfolios);
- Shape exchange-traded funds (ETFs), including ETFs aimed at both investing in the AI industry (Global X Robotics & Artificial Intelligence ETF) and using AI to make broad-based investment decisions (see Qraft AI-Enhanced U.S. Large Cap ETF); and
- Power actively managed stock funds (see Vanguard's use of AI in US$13 billion worth of quant stock funds).

But not everything AI is positive. The European Union approved a new artificial intelligence law to create a regulatory framework aimed at protecting consumers. And the International Monetary Fund recently discussed how AI's adoption in the financial services industry contains inherent risks, including embedded biases, privacy concerns, outcome opaqueness, unique cyberthreats, and the potential for creating new sources and transmission channels of systematic risks. Even Elon Musk has stated, on multiple occasions, that AI could be more dangerous to humanity than nuclear weapons.

Nearly every day, we hear about AI. What should fiduciaries be doing about it, if anything? The following are possible considerations:

- Is the current 3(21) investment advisor using AI appropriately (or inappropriately)?
- If there is a 3(38) investment manager, how much work is automated by AI, and does the plan sponsor understand the effect this may have on plan participants?
- What risks are associated with using (or not using) AI to help select investment options?
- What's the risk of misinformation or a biased output?
- Who is liable if the AI's advice leads to poor investment decisions?
- How does one evaluate the quality and accuracy of the content it produces? If the AI generates investment advice or market analysis for a 401(k) plan, how do fiduciaries ensure the information is reliable and compliant with regulations? There's a risk of misinformation or biased output, which could lead to poor investment decisions.
- If the 401(k) permits SDBAs, should it be limited to reducing risks associated with AI?
- Do the fiduciaries understand how the AI works, its biases, and the potential impact on investment decisions?
- Does the recordkeeper use AI to combat cybersecurity threats, communicate with participants, or for other purposes?
- Was a privacy or security assessment conducted on the AI systems? Vast amounts of sensitive participant data fuel these systems, making them prime targets for malicious actors seeking to exploit weaknesses in security protocols. A data breach or cyberattack could not only compromise the integrity of the retirement plan but also expose fiduciaries to legal and regulatory repercussions.
- Does the recordkeeper permit the Company to opt out of the use of AI?
- Are individual plan participants permitted to opt out of the use of AI?
- Do the benefits of AI-powered recordkeeping functions outweigh the potential risks?
- Should the Committee seek independent professional advice regarding what AI can provide to the Committee as a resource to satisfy fiduciary obligations under ERISA?

While AI may revolutionize 401(k) management, it does have its limitations and constraints. AI algorithms don't correctly account for unforeseen events and market fluctuations. While AI excels at analyzing historical data and identifying patterns, it may struggle to adapt to sudden changes or "black swan" events, leaving fiduciaries vulnerable to unexpected losses. Just like no two snowflakes or fingerprints are the same, the same is true with AI algorithms. Their capability is based on the quality and quantity of data available for training, resulting in vast differences in performance and reliability between AI algorithms. When data is limited, outdated, or biased, or where AI systems inadvertently perpetuate or amplify existing biases present in the data used for training, AI systems may produce unreliable or biased outcomes, skewed investment recommendations, and unequal treatment of plan participants, leading to suboptimal investment decisions. Fiduciaries must exercise caution when relying on AI-generated recommendations and ensure

that algorithms are trained on comprehensive and accurate data.

While AI may one day better understand human emotion, currently, the AI algorithms may lack the human intuition and judgment necessary to navigate complex investment landscapes effectively. While AI excels at processing vast amounts of data and identifying trends, it may struggle to incorporate qualitative factors, market sentiment, and subjective assessments into investment decisions.

There are no clear-cut answers to these questions, which is where the fiduciary decision-making process comes into play.

Fiduciary Decision-Making Risks and Potential Liabilities

As every plan sponsor involved in 401(k) fee litigation knows, one of the most critical factors in ERISA litigation is the process. On the one hand, the process can be tantamount to mounting a defense, getting a lawsuit dismissed in the early stages, and reducing potential settlements. On the other hand, failure to follow a documented process can lead to expensive litigation, large settlements, and the perception of impropriety coupled with reputational damage, even if the underlying ERISA claim is largely without merit.

AI may also be used to sue a plan's sponsors and fiduciaries. If the 401k fee litigation roadmap is followed, AI-related claims will attack the fiduciary decision-making process, or lack thereof, by claiming that plan participants were hurt by fiduciaries' neglect of, indifference to, or lack of competency regarding AI's impact on the retirement plan industry. Unlike traditional investment strategies, where decisions are made based on clear, understandable criteria, AI algorithms often operate as "black boxes," making it challenging for fiduciaries to understand and justify the rationale behind AI-generated recommendations. This lack of transparency can erode trust and confidence in the retirement plan among participants and regulators, potentially creating litigation exposure. Claims may allege investment performance suffered compared to other plans that used (or didn't use) AI, and plan participants would have been better off if the recordkeeper used (or did not use) AI for cybersecurity, participant communications, other vital plan functions, or other novel claims. The underlying lawsuits will take a shotgun approach, even if there is little to no basis for the underlying claims. The goal is to get to discovery in the hopes of discovering a process problem and extracting a costly settlement.

Solutions

Integrating AI in 401(k) plan management presents opportunities and challenges for fiduciaries. While AI has the potential to revolutionize decision-making processes and improve participant outcomes, it also introduces new risks and limitations that must be addressed.

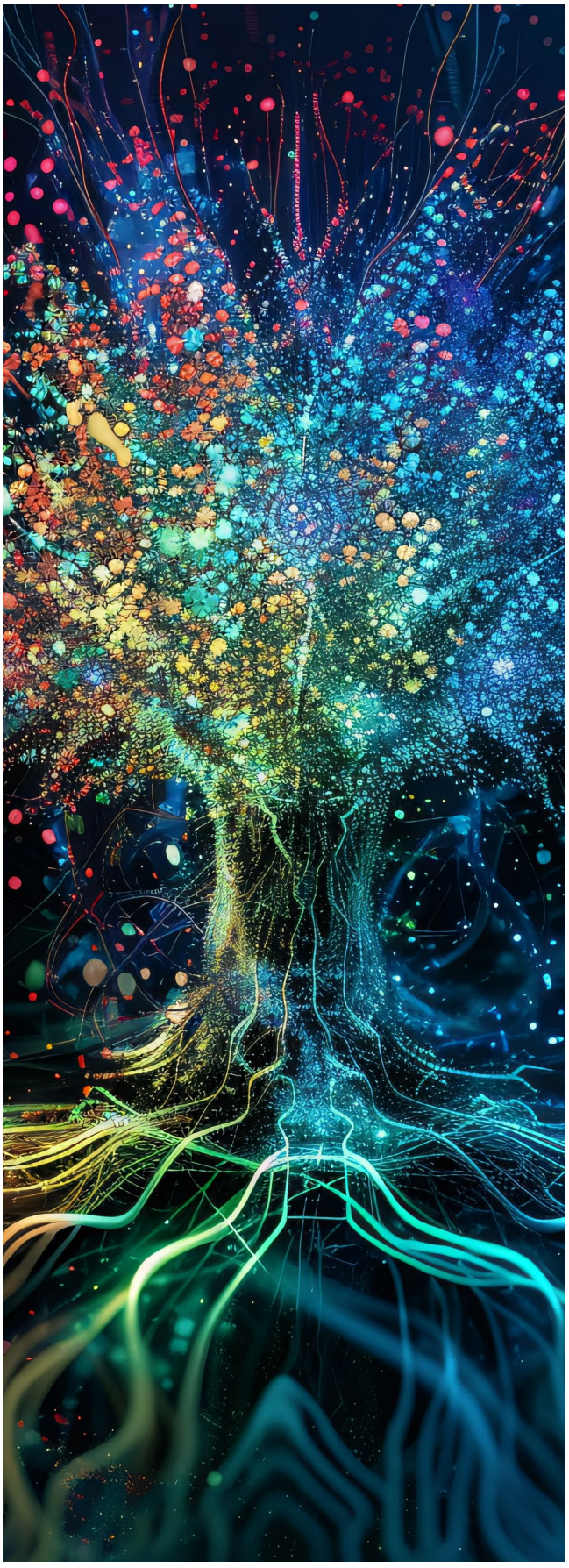
For ERISA litigation, we believe the actual decision to use (or not use) AI will take a backseat to whether plan fiduciaries had a process to evaluate AI issues and whether that process was followed. Ultimately, fiduciaries may need to weigh the benefits against the risks associated explicitly with using (or not using) AI. Potential solutions include:

- Stipulating the evaluation of AI in the Committee's chartered duties. This includes defining clear roles and responsibilities for stakeholders involved in AI implementation, conducting regular audits and assessments of AI systems to ensure compliance with regulatory requirements and best practices, and implementing mechanisms for monitoring and mitigating algorithmic bias;
- Questioning (and documenting the questioning) of the plan's 3(21) advisor's or 3(38) manager's use of and options related to AI. Fiduciaries must prioritize transparency and accountability, which includes documenting and disclosing the methodologies and assumptions underlying AI algorithms, as well as providing plan participants with clear explanations of how AI is utilized in investment decision-making processes;
- Evaluating current recordkeeper AI capabilities, risks, and options;
- Educating, training, and equipping fiduciaries with the knowledge and skills necessary to evaluate and leverage AI effectively. This includes staying informed about advancements in AI technology, understanding the potential risks and limitations associated with AI, and cultivating a culture of ethical and responsible AI usage;

- Reviewing plan service provider contracts for any AI-specific provisions or any AI-related liability shifting or disclaimers;
- Assessing cybersecurity and data privacy protocols, policies, and procedures to protect against potential threats and vulnerabilities associated with AI systems, implementing robust cybersecurity measures, such as encryption, access controls, and intrusion detection systems, to safeguard sensitive participant information and prevent unauthorized access or tampering with AI algorithms;
- When running an RFP for a new recordkeeper, ask a few AI-related questions;
- Considering that rather than replacing human expertise, AI could be viewed as a complement to human judgment and intuition. Fiduciaries could leverage AI tools and algorithms to augment, rather than replace, human decision-making processes and develop more robust and well-informed investment strategies that account for a broader range of factors and considerations;
- Obtaining or increasing fiduciary liability insurance coverage; or
- Doing nothing (which, for some, may be the best option).

The 401k fee litigation has taught us that not having a process or omitting an analysis is bad. Deviating from a documented process is disastrous. Depending on the size of the plan, the sophistication of fiduciaries, and the current participant mix, it may or may not be appropriate for fiduciaries to take specific action related to AI.

Given the current trajectory of AI, AI-related issues will likely become a part of the fiduciary decision-making process or, at a minimum, influence decisions, requiring fiduciaries to remain vigilant and proactive in adapting to the changes brought on by AI as it continues to evolve and mature. As AI continues to evolve and mature, fiduciaries must remain vigilant and proactive in adapting to the changing landscape of retirement planning to ensure the long-term success and sustainability of 401(k) plans.



A Look at the Evolving Scope of Transatlantic AI Regulations

AUTHORS

Natasha Allen | nallen@foley.com

David Kantaros | dkantaros@foley.com

Published August 2024 by Foley & Lardner LLP

There have been significant changes to the regulations surrounding artificial intelligence (AI) on a global scale. New measures from governments worldwide are coming online, including the United States (U.S.) government's executive order on AI, California's upcoming regulations, the European Union's AI Act, and emerging developments in the United Kingdom that contribute to this evolving environment.

The European Union (EU) AI Act and the U.S. Executive Order on AI aim to develop and utilize AI safely, securely, and with respect for fundamental rights, yet their approaches are markedly different. The EU AI Act establishes a binding legal framework across EU member states, directly applies to businesses involved in the AI value chain, classifies AI systems by risk, and imposes significant fines for violations. In contrast, the U.S. Executive Order is more of a guideline as federal agencies develop AI standards and policies. It prioritizes AI safety and trustworthiness but lacks specific penalties, instead relying on voluntary compliance and agency collaboration.

The EU approach includes detailed oversight and enforcement, while the U.S. method encourages the adoption of new standards and international cooperation that aligns with global standards but is less prescriptive. Despite their shared objectives, differences in regulatory approach, scope, enforcement, and penalties could lead to contradictions in AI governance standards between the two regions.

There has also been some collaboration on an international scale. Recently, there has been an effort between antitrust officials at the U.S. Department of Justice (DOJ), U.S. Federal Trade Commission (FTC), the European Commission, and the UK's Competition and Markets Authority to monitor AI and its risks to competition. The agencies have issued a joint statement, with all four antitrust enforcers pledging to "to remain vigilant for potential competition issues" and to use the powers of their agencies to provide safeguards against the utilization of AI to undermine competition or lead to unfair or deceptive practices.

The regulatory landscape for AI across the globe is evolving in real time as the technology develops at a record pace. As regulations strive to keep up with the technology, there are real challenges and risks that exist for companies involved in the development or utilization of AI. Therefore, it is critical that business leaders understand regulatory changes on an international scale, adapt, and stay compliant to avoid what could be significant penalties and reputational damage.

The U.S. Federal Executive Order on AI

In October 2023, the Biden Administration issued an executive order to foster responsible AI innovation. This order outlines several key initiatives, including promoting ethical, trustworthy, and lawful AI technologies. It also calls for collaboration between federal agencies, private companies, academia, and international partners to advance AI capabilities and realize its myriad benefits. The order emphasizes the need for robust frameworks to address potential AI risks such as bias, privacy concerns, and security vulnerabilities. In addition, the order directs that various sweeping actions be taken, including the establishment of new standards for AI safety and security, the passing of bipartisan data privacy legislation to protect Americans' privacy from the risks posed by AI, the promotion of the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges, and

the implementation of actions to ensure responsible government deployment of AI and modernization of the federal AI infrastructure through the rapid hiring of AI professionals.

At the state level, Colorado and California are leading the way. Colorado enacted the first comprehensive regulation of AI at the state level with The Colorado Artificial Intelligence Act (Senate Bill (SB) 24-205), signed into law by Governor Jared Polis on May 17, 2024. As our team previously outlined, The Colorado AI Act is comprehensive, establishing requirements for developers and deployers of "high-risk artificial intelligence systems," to adhere to a host of obligations, including disclosures, risk management practices, and consumer protections. The Colorado law goes into effect on February 1, 2026, giving companies over a year to thoroughly adapt.

In California, a host of proposed AI regulations focusing on transparency, accountability, and consumer protection would require the disclosure of information such as AI systems' functions, data sources, and decision-making processes. For example, AB2013 was introduced on January 31, 2024, and would require that developers of an AI system or service made available to Californians to post on the developer's website documentation of the datasets used to train the AI system or service.

SB970 is another bill that was introduced in January 2024 and would require any person or entity that sells or provides access to any AI technology that is designed to create synthetic images, video, or voice to give a consumer warning that misuse of the technology may result in civil or criminal liability for the user.

Finally, on July 2, 2024, the California State Assembly Judiciary Committee passed SB-1047 (Safe and Secure Innovation for Frontier Artificial Intelligence Models Act), which regulates AI models based on complexity.

The European Union's AI Act

The EU is leading the way in AI regulation through its AI Act, which establishes a framework and represents Europe's first comprehensive attempt to regulate AI. The AI Act was adopted to promote the uptake of human-centric and trustworthy AI while ensuring high level protections of health, safety, and fundamental rights against the harmful effects of AI systems in the EU and supporting innovation.

The AI Act sets forth harmonized rules for the release and use of AI systems in the EU; prohibitions of certain AI practices; specific requirements for high-risk AI systems and obligations for operators of such systems; harmonized transparency rules for certain AI systems; harmonized rules for the release of general-purpose AI models; rules on market monitoring, market surveillance, governance, and enforcement; and measures to support innovation, with a particular focus on SMEs, including startups.

The AI Act classifies AI systems into four risk levels: unacceptable, high, limited, and minimal. Applications that pose an unacceptable risk, such as government social scoring systems, are outright banned. High-risk applications, including CV-scanning tools, face stringent regulations to ensure safety and accountability. Limited risk applications lack full transparency as to AI usage, and the AI Act imposes transparency obligations. For example, humans should be informed when they are using AI systems (such as chatbots) that they are interacting with a machine and not a human so as to enable the user to make an informed decision whether or not to continue. The AI Act allows the free use of minimal-risk AI, including applications such as AI-enabled video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.

The adoption of the AI Act has not come without criticism from major European companies. In an open letter signed by 150 executives, they raised concerns over the heavy regulation of generative AI and foundation models. The fear is that the increased compliance costs and hindered productivity would drive companies away from the EU. Despite these concerns, the AI Act is here to stay, and it would be wise for companies to prepare for compliance by assessing their systems.

Recommendations for Global Businesses

As governments and regulatory bodies worldwide implement diverse AI regulations, companies have the power to adopt strategies that both ensure compliance and mitigate risks proactively. Global businesses should consider the following recommendations:

1. **Risk Assessments:** Conducting thorough risk assessments of AI systems is important for companies to align with the EU's classification

scheme and the U.S.'s focus on safety and security. There must also be an assessment of the safety and security of your AI systems, particularly those categorized as high-risk under the EU's AI Act. This proactive approach will not only help you meet regulatory requirements but also protect your business from potential sanctions as the legal landscape evolves.

2. **Compliance Strategy:** Develop a compliance strategy that specifically addresses the most stringent aspects of the EU and U.S. regulations.

3. **Legal Monitoring:** Stay on top of evolving best practices and guidelines. Monitor regulatory developments in regions in which your company operates to adapt to new requirements and avoid penalties and engage with policymakers and industry groups to stay ahead of compliance requirements. Participation in public consultations and industry forums can provide valuable insights and influence regulatory outcomes.

4. **Transparency and Accountability:** To meet ethical and regulatory expectations, transparency and accountability should be prioritized in AI development. This means ensuring AI systems are transparent, with clear documentation of data sources, decision-making processes, and system functionalities. There should also be accountability measures in place, such as regular audits and impact assessments.

5. **Data Governance:** Implement robust data governance measures to meet the EU's requirements and align with the U.S.'s emphasis on trustworthy AI. Establish governance structures that ensure compliance with federal, state, and international AI regulations, including appointing compliance officers and developing internal policies.

6. **Invest in Ethical AI Practices:** Develop and deploy AI systems that adhere to ethical guidelines, focusing on fairness, privacy, and user rights. Ethical AI practices ensure compliance, build public trust, and enhance brand reputation.

Old Employment Law Principles Can Answer New AI Concerns

AUTHOR

Mark Neuberger | mneuberger@foley.com
John Litchfield | jlitchfield@foley.com
Michael Ryan | mryan@foley.com

Published September 2024 by Foley & Lardner LLP

This article was originally published in Law360 on September 6, 2024, and is republished here with permission.

The integration of artificial intelligence into the workplace has sparked a flurry of legal and regulatory discussions in recent months.

Judges are instituting bans and other regulations on the use of AI in courts. States are passing laws designed to curb or control the use of AI in employment-related policies and decision making. And employers are grappling with how existing employment laws apply to a rapidly evolving and diverse offering of AI tools.

While AI introduces new technological dimensions to the employment landscape, the core legal issues raised by the use of AI are not new. Rather, AI is the metaphorical remake on a classic, where familiar employment law concerns are simply repackaged and recontextualized within a shiny new technological framework.

Employers — particularly those that not that long ago may have had to Google what AI even was — should take comfort that AI, and the burgeoning laws and regulations that surround it, most often reflect familiar and long-standing legal issues, albeit with a modern twist.

Discrimination and Fair Employment Practices

Whether AI is involved or not, the heart of many employment law concerns is the issue of discrimination. Traditional employment laws, such as Title VII of the Civil Rights Act, prohibit employers from discriminating in the hiring and selection process based on race, color, religion, sex, and national origin.

With the advent and rapid implementation of AI in companies across the country, these principles continue to be relevant, but with slightly increased complexity where employers are now integrating AI tools and data to support the recruitment and hiring decision-making process. But what really has changed?

As with the risk for human error in decision making generally, AI systems are made by humans, and the AI tools used in hiring and recruitment have the potential to perpetuate or even exacerbate human biases if the AI tools are not carefully designed, monitored, and validated.

For instance, if an AI system is trained on historical data that reflects past hiring biases, it can replicate and reinforce these biases in its decision-making processes despite facially appearing to be based purely on objective metrics and data. Without validation, this can result in discriminatory outcomes that unfairly disadvantage certain protected groups of persons, leading to potential violations of antidiscrimination laws.

AI merely reinforces the eternal need for employers to trust but verify.

The U.S. Equal Employment Opportunity Commission and other enforcement agencies have recently warned that AI selection tools may have implicit or actual bias built into their systems, but this should not be news to employers. In 1978, the EEOC, U.S. Department of Labor and U.S. Department of Justice jointly issued a very comprehensive set of regulations called the Uniform Guidelines on Employee Selection Procedures, or UGESP, which was designed to ensure that all selection devices and procedures are not used in a discriminatory manner.

The reach of the UGESP is extremely broad. At the time, it was focused on paper and pencil tests used in making any employment-related decisions because there was a long history of many of these tests having a disparate impact on protected groups without much scientific proof they actually predicted successful performance on the job. AI doesn't change this dimension of employment law, it merely expands it to a new frontier, as the UGESP remains in effect today.

Disparate impact concerns underpin AI-related regulations across the country, which often seek transparency with respect to the data and inputs used to create or guide the AI in making decisions. But instead of looking at the wide-ranging regulations and seeing a paradigm shift in the way employee recruitment works, employers can take heart that what's going on is really just a new way of looking at an old problem.

Essentially, most of the new AI regulations ask questions that previously needed to be asked of hiring managers: Where is the source data coming from? Who is doing the interpretation? Is the decision, and underlying data, valid and objective?

Answers to these questions do not depend on or change based on whether AI was involved at some point in the decision-making process. In short, employers don't need to do anything conceptually different, they just need to learn the new tools — and how the same old problems can arise with those new tools — to ensure those problems are addressed beforehand.

Privacy and Data Protection

Privacy concerns are another area where traditional employment laws intersect with AI technology.

Historically, employment laws have mandated the protection of employees' personal information. With the proliferation of AI, which often relies on large datasets to function effectively, the volume and sensitivity of data collected have increased significantly. But the increase in volume and sensitivity changes nothing about the underlying legal risks and concerns that are addressed by prevailing employer conduct today.

Just as data breaches can occur from the general storage and maintenance of personal information, so too can AI be breached. The underlying concerns don't change. In essence, while the technology has changed, the fundamental issue remains: ensuring that employees' personal information is protected and used in a manner consistent with established privacy laws. Employers just have to keep on trucking by adding AI-related apps and tools to the list of data sources they already monitor for compliance.

The same goes for protecting an employer's confidential and proprietary information.

Employers have historically protected their own sensitive data by obligating employees to enter into confidentiality agreements, or by promulgating employment policies regarding the same, then notifying employees regarding the employer's active or random monitoring of employee activity while using electronic equipment. Employee use of AI technologies for work-related reasons, particularly those AI tools that are web-based and not internally captive to the employers, merely increases the risk that sensitive confidential and proprietary information is leaked to the public.

Reviewing, updating, and training on existing policies and agreements to warn employees of these risks, and the consequences for not being mindful of their use of AI for work, is key to mitigating the odds of an unfortunate and costly leak. Such training should already be ongoing outside the AI paradigm.

Employment Classification and Job Security

Employment classification, which determines whether workers are classified as employees or independent contractors, has also been a long-standing issue in employment law. This classification affects workers' rights to benefits, job security, and protections under labor laws. The rise of AI and automation introduces new dimensions to this topic.

Specifically, AI and automation can lead to shifts in job roles and functions, raising questions about how workers should be classified. For example, if an AI system performs tasks traditionally done by employees, does this change the nature of the employee's employment or the primary duty they perform as regulated by established classification tests? There are also concerns about job displacement and the need for new types of worker protections as AI systems become more prevalent.

But "Death of Jobs in America Based on Advent of New Technology" is not a new headline in 2024

and has not been a new addition to the employment landscape at any point in the last century. AI may work differently from certain past technological innovations, but the fundamental challenges it poses do not. AI encompasses a wide-ranging set of tools employers can use to aid their operations, but those tools still require human operation, monitoring, and validation.

Employers should think carefully about how best to integrate AI into their existing operations, keeping in mind all the same worker classification issues that they had to worry about well before the term "AI" reached their ears.

Workplace Health and Safety

Workplace health and safety regulations have traditionally focused on protecting employees from physical harm. As AI systems become more integrated into the workplace, new safety considerations emerge. For instance, the deployment of robots and automated machinery requires rigorous safety standards to prevent accidents and injuries.

Furthermore, the use of AI in the monitoring and managing of workplace conditions, such as ergonomics or environmental factors, raises questions about how these technologies affect workers' well-being. Ensuring that AI systems are designed and implemented with safety in mind is crucial for maintaining a safe work environment, but it does not fundamentally alter the legal landscape and risk factors embedded in this common litigation risk factor in the workplace.

Takeaways

In sum, while the rise of AI introduces new challenges and considerations into employment law, many of these issues are simply existing legal concerns repackaged within a technological framework. Discrimination, privacy, employment classification, and workplace safety have always been central to employment law, and AI does not fundamentally alter these issues but rather highlights their continued relevance with a new technological spin.

Employers should carefully scrutinize any use of AI in selection, promotion, or other employment decisions, which should be a mere continuation of such scrutiny with respect to the validity of the test as it applies to the employer's workplace and the specific jobs for which the test is applicable. The consequences of using a selection device that has an adverse impact without an appropriate validation study can be severe, which was the case long before AI entered the mainstream.

As AI technology continues to evolve, it is essential for legal frameworks to adapt and address the specific nuances introduced by AI, but the underlying principles of fairness, privacy, and protection that have guided employment law for decades remain as pertinent as ever. The challenge for regulators and employers will be to ensure that these principles are upheld in the face of new technological advancements, ensuring that the benefits of AI can be realized while maintaining robust protections for workers.

Employers, you can breathe a sigh of relief. Technology is changing, but the legal compliance regimes you have established do not have to be fundamentally rebuilt from the ground up. What's old is just new again, and everybody loves a classic.

Contributors

Michael Abbott

Partner
+1 713 276 5571 | mabbott@foley.com
Houston

Natasha Allen

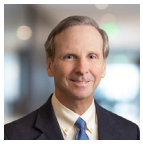
Partner
+1 650 251 1112 | nallen@foley.com
Silicon Valley

James De Vellis

Partner
+1 617 342 4037 | jdevellis@foley.com
Boston

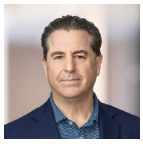
Peter Fetzer

Partner
+1 414 297 5596 | pfetzer@foley.com
Milwaukee



Chanley Howell

Partner
+1 904 359 8745 | chowell@foley.com
Jacksonville



David Kantaros

Partner
+1 617 342 4068 | dkantaros@foley.com
Boston

Louis Lehot

Partner
+1 650 251 1222 | llehot@foley.com
Silicon Valley

John Litchfield

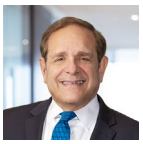
Partner
+1 312.832.4538 | jlitchfield@foley.com
Chicago

James Lundy

Partner
+1 312 832 4992 | jglundy@foley.com
Chicago

Aaron Tantleff

Partner
+1 312 832 4367 | atantleff@foley.com
Chicago



Mark Neuberger

Of Counsel
+1 305 482 8408 | mneuberger@foley.com
Miami

Austin Kim

Senior Counsel
+1 617 502 3295 | akim@foley.com
Boston

Michael Ryan

Senior Counsel
+1 713.276.5175 | mryan@foley.com
Houston

Abdullah Akhtar

Associate
+1 617 226 3147 | aakhtar@foley.com
Boston

William McCaughey

Associate
+1 212 338 3425 | wmccaughey@foley.com
New York

Randy Pummill

Associate
+1 214 999 4049 | rpummill@foley.com
Dallas

Cullen Werwie

Associate
+1 608 258 4322 | cwerwie@foley.com
Madison

ABOUT FOLEY & LARDNER LLP

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care, and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI | MILWAUKEE
NEW YORK | ORLANDO | RALEIGH | SACRAMENTO | SALT LAKE CITY | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.