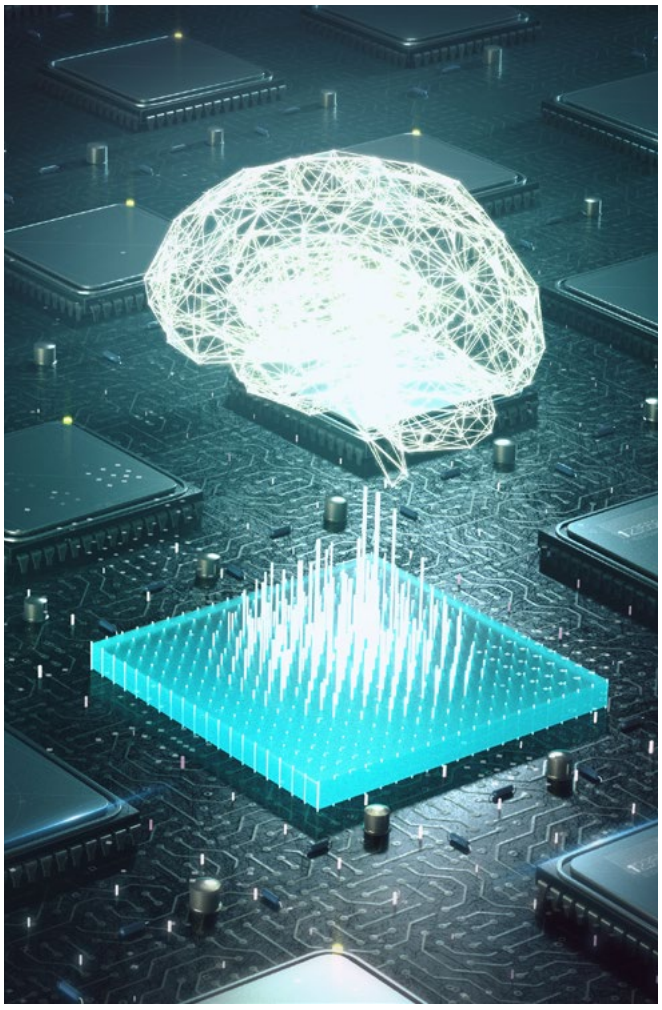
HUNTON
ANDREWS KURTH

SPRING 2024

AI and Emerging Technologies

CONTRACTING AND VENDOR MANAGEMENT

Shaping the Future: Ensuring Responsible AI Use through Vendor Policies and Procedures



Over the last several years, the astounding improvements and capabilities in artificial intelligence (AI) technology has made AI integral to everyday business functions. According to Forbes in its 2023 article "24 Top AI Statistics And Trends In 2024," the market value of AI is expected to skyrocket to $407 billion by 2027, with an expected annual growth rate of 37.3 percent.[1] This research suggests that more and more companies will only increase their reliance on these technologies, with an estimated 64 percent of businesses expecting artificial intelligence to increase their workforce productivity.[2] From customer service to accounting, fraud detection, and predictive analysis, AI has proven that expectation correct and reshaped the industries as we knew them. In an era propelled by the transformative potential of AI, the need for comprehensive policies and procedures governing its use has never been more pressing. Through collaboration and proactive measures, both companies and their vendors can navigate the evolving landscape of AI with confidence and integrity.

Although you and your company may be rushing to establish policies and procedures for the responsible use of AI, don't neglect to ask your vendors how they are handling AI and if they have policies and procedures for the use of AI. It's imperative not to overlook the practices of your vendors, especially if you believe, or even expect, that they will use AI tools in the provision of professional services, including deliverables, to you. In virtually all industries, but certainly in the creative arts and writing, the consensus is that the use of AI is inevitable. If this is true, you and your company can

1 Katherine Haan and Rob Watts, 24 Top AI Statistics And Trends, Forbes (Apr. 25, 2023).

2 Katherine Haan and Rob Watts, 24 Top AI Statistics And Trends, Forbes (Apr. 25, 2023).

expect that the marketers, advertisers, agencies, consultants and yes, even lawyers, that you hire are likely to be utilizing AI tools to deliver your work product.

Instead of reinventing the wheel when it comes to addressing AI with your vendors, companies can rely on expanding existing safeguards. Even before the era of AI, common place vendor requirements included requirements that vendors comply with a company's Supplier Code of Conduct. Supplier Codes of Conduct often address a broad range of topics from anti-bribery to sanctions compliance, support of environmental protection, climate change mitigation and support for diversity and inclusion. Likewise, the Supplier Code of Conduct and similar contract documents can also address whether vendors use AI and whether they have industry standard policies and procedures in place pertaining to their use of AI. Further, due diligence questions addressed to new vendors and new vendor onboarding processes already ask for a broad range of information designed to ensure vendors are qualified and meet certain standards. Such due diligence and onboarding processes should also include questions about the vendor's use of AI and whether the vendor has established and maintains policies and procedures geared specifically to the use of AI.

So, if you and your company would like to inquire about how vendors are using AI and if they have policies and procedures in place pertaining to AI, what might you expect? And, if you have the opportunity to ask a vendor to establish a policy or procedure, what might you require of such policy or procedure? While there are certainly many different possible approaches depending on the context, we have several suggestions.

First, you may want to require a vendor to have a written policy, or to establish a written policy by a certain date. Given the current scramble to establish AI-related policies, and the sense many of us have that to the industry doesn't yet understand the full capability and impact of AI and its use cases, consider maintaining some level of flexibility in requiring a policy by a certain date, and, instead, require periodic review and updates to the policy as the technology evolves.

Second, you may want to require a vendor to have a c-suite executive or committee tasked with developing policies and procedures on the use of AI for the company, its personnel and its vendors. Without strong support from upper management, a vendor will likely have personnel using AI at various levels of the company without adequate oversight. This may prove difficult as many employees may already be using AI without disclosing their use to management. Indeed, a study by professional social network Fishbowl in February 2023 revealed that, 68 percent of 5,067 respondents who used AI at work reported that they do not disclose their AI use to their bosses.[3] As workplace bans on AI increase, so do online forums centered around secretly circumventing these bans either through high-tech solutions like integrating ChatGPT into a native app disguised as a workplace tool, or through more basic methods such as using the AI tools on their personal phone or using privacy screens on their computers.[4]

Third, in order to address this concern, you may want to require a vendor to establish an employee training program designed to ensure employees and other personnel are aware of the company's AI policies, what safeguards they

3 Alex Christian, The employees secretly using AI at work, BBC (Oct. 24, 2023).

4 Alex Christian, The employees secretly using AI at work, BBC (Oct. 24, 2023). See also, r/GodSpeed46, r/ChatGPTOPro, Seeking Solutions to Use ChatGPT Discreetly at Work - Ideas Needed!, Reddit (April 24, 2023); u/PaypayaEqual, r/ChatGPT, My company blocked chatgpt, Reddit (Jan. 6, 2023)

should employ, how they might need to document their use of AI, as well as any output review, fact-checking or other actions that should be taken to ensure AI output is analyzed and reviewed by humans.

Finally, if you do require your vendors to provide its AI policies and procedures to you as part of standard diligence, or contractually require vendors to establish and maintain (and update) AI policies, you may also want to consider whether certain vendors should deliver any documentation to you on the distinct use of AI related to specific deliverables or services. If you believe AI may be used in the creation of a deliverable, you may want to require certifications or other documentation to indicate that the vendor's employees have received appropriate training and used AI in accordance with the vendor's policies and procedures. While we suspect that such requirements would be over-broad and over-bearing in many cases, there may be some critical services where such a process would be useful and perhaps even necessary.

There is no greater cautionary tale for the need for comprehensive AI policies and procedures than the recent surge of AI-related controversies in the legal industry. In the last year alone, several lawyers have had to explain to their state's bar association why cases submitted in their legal briefs, sourced from generative AI websites, do not seem to exist.[5] Earlier this year, Michael Cohen's lawyers landed themselves in hot water after he provided fake case citations generated by Google Bard, an AI platform, which were later submitted to a federal court in New York.[6] In another recent instance, attorneys from a prominent special education law firm received criticism from a judge after partially basing their legal fees on advice from ChatGPT.[7] These stories underscore the potential risks and pitfalls for legal authorities and businesses alike when AI is employed without proper oversight. Consequently, legal authorities, including state bar associations, have begun issuing standardized guidelines on how and in what manner attorneys can interact with artificial intelligence.[8] As legal authorities begin to implement standardized guidelines for attorneys' interaction with AI, it becomes evident that similar frameworks are necessary for companies and vendors across various industries.

So, what does AI think about this article? We asked and AI provided this summary and conclusion: By establishing robust governance frameworks and mechanisms for oversight, companies and vendors can harness the full potential of AI while mitigating risks and safeguarding against potential misuse.

Sharon Palmer Harrington
Counsel, Richmond

Jaime E. Bloxom
Associate, Richmond

Asha McCorvey
Law Clerk, Richmond

5 Sara Merken, Another NY lawyer faces discipline after AI chatbot invented case citation, AP News (Jan. 30, 2024).

6 David Thomas, Michael Cohen's lawyer asks court to spare sanctions over made-up cases, AP News (Jan. 3, 2024).

7 Chris Dolmstech, Lawyers Use ChatGPT to Add Up Fees, Judge Faults Their Math (Feb. 22, 2024).

8 Sarah Merken, New York lawyers urged to use AI with care in new state bar guidelines, AP News (Apr. 8, 2024).

INTELLECTUAL PROPERTY

The USPTO's Useful New AI-Assisted Invention Guidance: What Does It Mean?

The US Patent and Trademark Office (USPTO) recently released its Inventorship Guidance for AI-Assisted Inventions, providing inventors and patent applicants with a framework regarding artificial intelligence-assisted inventions and how such will be judged at the USPTO. 89 Fed. Reg. 10043 (Feb. 13, 2024). The guidance—a needed clarifying guidepost along the AI road—is effective immediately.

The Human Inventorship Requirement Remains

The first, and perhaps most critical, takeaway from the new guidance is that the human inventorship requirement remains unchanged. Inventions created *entirely* by AI are still unpatentable.

However, the guidance allows for the patenting of inventions created jointly between man and machine, provided the human(s) "significantly contributed to the invention." 89 Fed. Reg. at 10046. That is, a person has to do more than merely rely upon an AI system to come up with an invention. Further, only natural person(s) may be named as inventor(s) on the patent application submitted to the USPTO, and any subsequent patent that issues.

What Is a Significant Contribution? No Bright-Line Test

This standard for inventorship is not new, but does raise the question: what qualifies as a "significant contribution" to an invention in the context of an AI-assisted invention?

The USPTO recognizes that determining whether a contribution is significant could be difficult, and notes that—like in many areas of the law—there is not a bright-line test. However, it does provide a list of "guiding principles" to help aid the determination:

1. A natural person's use of an AI system in creating an AI-assisted invention does not negate the person's contributions as an inventor.
2. A natural person's mere recognition of a problem or having a general goal or research plan to pursue does not rise to the level of conception. However, a significant contribution could be shown by the way the person constructs the prompt in view of a specific problem to elicit a particular solution from the AI system.

3. A natural person's mere recognition and appreciation of the output of an AI system as an invention and subsequent reduction to practice alone is not a significant contribution that rises to the level of inventorship.
4. A natural person who develops an essential building block from which the claimed invention is derived may be considered to have provided a significant contribution to the conception of the claimed invention even though the person was not present for or a participant in each activity that led to the conception of the claimed invention.
5. Maintaining 'intellectual domination' over an AI system does not, on its own, make a person an inventor of any inventions created through the use of the AI system.

89 Fed. Reg. at 10048-49. The USPTO also issued two examples with the guidance that present different scenarios with analysis regarding determination of inventorship, one called "Transaxle for Remote Control Car" and one called "Developing a Therapeutic Compound for Treating Cancer." *See* Fed. Reg. at 10045. The examples serve to illustrate application of the guiding principles.

A Contribution to Every Claim

The guidance makes clear that a human must significantly contribute to *each claim* in the patent application. Essentially, a human may not invent a single independent claim and then allow the AI to take over. For example, we can imagine a scenario in which the AI develops refinements that lead to multiple other claims stemming from the one independent claim. The human may not file a patent application on those other claims naming itself as an inventor of those AI-created claims. The assessment for inventive contribution applies to all claims.

What is less clear is how the interaction between *dependent and independent* claims will be viewed, where the independent claim originated from a human, but the dependent claims that offer further specificity were developed by AI.

As with Copyright Law, AI May Be Used as a Tool for Patents

The guidance signals that AI may be used as a tool to aid—but not replace—human contribution in patents. This is consistent with the authorship requirement of copyright law. Indeed, a direct parallel exists, where the copyright term "author" is interpreted to mean "human author," as seen in the now-infamous "monkey selfie" case, which held that a monkey could not own the copyright in a photograph it took. *Naruto v. Slater, et al.*, 888 F.3d 418 (9th Cir. 2018). The guidance is also consistent with positions of the courts and US Copyright Office, which have determined that the mere presence of AI in the creation of a work does not doom a copyright application, but any material created by AI must be disclaimed by the human author. *See, e.g., Thaler v. Perlmutter, et al.*, No. 22-1564 (BAH), 2023 WL 5333236 (D. D.C., Aug. 18, 2023).

Future Challenges and Takeaways

While the guidance only just issued, and clearly will face challenges and questions with future application, this was a crucial step from the USPTO to clarify this evolving technological area.

The key takeaway for patent applicants and in-house IP legal teams is that, while humans remain central to the inventorship of patentable ideas, AI tools can be used to assist in the invention development process. However, such tools should be used with caution. Personnel using AI tools need to understand the required role of the human in an invention. That role goes beyond merely prompting the AI to produce a result and submitting it as an invention in a patent application to the USPTO.

In-house legal personnel, along with outside counsel, must evaluate what role the human played in the invention process to ensure that inventorship is proper for submission to the USPTO.

Steven L. Wood
Counsel, Washington, DC

LABOR AND EMPLOYMENT

New York and California: Technology and AI Updates for Employers

New York Restricts Employers Use of Social Media

A New York law prohibiting employers from accessing employees' or job applicants' *personal* social media accounts went into effect in March. Under the new legislation, "personal accounts" are broadly defined to mean "an account or profile on an electronic medium where users may create, share, and view user-generated content, including uploading or downloading videos or still photographs, blogs, video blogs, podcasts, instant messages, or internet website profiles used exclusively for personal purposes."

The new law makes it unlawful for an employer to request, require or coerce an employee or applicant to: (i) disclose the username, password or "other authentication information" for accessing personal accounts; (ii) access "personal account in the presence of the employer"; or (iii) "reproduce in any manner photographs, videos, or other information contained within a personal account" obtained by the prohibited means in (i) and (ii). Employers are prohibited from retaliating against an employee or applicant who refuses to provide personal account access information to an employer that unlawfully requests it.

There are a few exceptions to New York's sweeping prohibition on accessing employee and applicant social media accounts. First, if an employee or applicant voluntarily adds the employer to their list of contacts associated with a personal account, then the employer is not prohibited from accessing the account. Second, an employer may require employees to disclose the username, password or other authenticating information for non-personal accounts that "provide access to the employer's internal computer or information systems," such as through a link to the employer's intranet or internal database. Third, employers can still require that employees disclose access information to an account provided by the employer for business purposes and access an electronic communications device paid for by the employer, so long as the employee was provided prior notice of the employer's right to request such access and the provision of the device was conditioned on the employer's right to access it. Notably, however, employers are still prohibited from accessing personal accounts on devices it paid for.

Finally, the new legislation does not restrict employers from viewing, accessing or utilizing information: (i) "about an employee or applicant that can be obtained without any required access information"; (ii) "that is available in the public domain"; or (iii) "for the purposes of obtaining reports of misconduct or investigating misconduct, photographs, video, messages, or other information that is voluntarily shared by an employee, client, or other third party that the employee subject to such report or investigation has voluntarily given access to contained within such employee's personal account."

State Regulation of AI – California Continues Wave of AI Legislation

With the tremendous growth in AI use, concerns have arisen about its potential to discriminate against individuals when it's used in critical decision-making processes in sectors such as employment, housing and credit. In response to these growing concerns, California has introduced Assembly Bill 2930 (AB 2930) on February 15, 2024. AB 2930 seeks to combat "algorithmic discrimination" by introducing a series of regulations intended to make AI more transparent, fair and accountable.

"Automated decision tools" are at the center of AB 2930 and are defined as any system using AI that has been developed to make, or be a controlling factor in making, "consequential decisions." A "consequential decision" is defined as a decision or judgment that has a legal, material or similarly significant effect on an individual's life relating to:

1) employment; 2) education; 3) housing or lodging; 4) essential utilities; 5) family planning; 6) adoption services, reproductive services or assessments related to child protective services; 7) health care or health insurance; 8) financial services; 9) the criminal justice system; 10) legal services; 11) private arbitration; 12) mediation; and 13) voting.

AB 2930 imposes requirements on not only those who develop automated decision tools, but also those who deploy automated decision tools, such as employers. The requirements include impact assessments, notice requirements, governance programs, policy disclosure requirements and liability and penalties for non-compliance.

IMPACT ASSESSMENTS

Any employers or developers using or developing automated decision tools will be required to perform annual impact assessments by January 1, 2026. The annual impact assessment requirements are largely the same for both employers and developers and include a statement of purpose for the automated decision tool; descriptions of the automated decision tool's outputs and how they are used in making a consequential decision; and analysis of potential adverse impacts. Employers, but not developers, are required to describe the safeguards in place to address reasonably foreseeable risks of algorithmic discrimination and provide a statement of the extent to which the employer's use of the automated decision tool is consistent with or varies from the developer's statement of the intended use of the automated decision tool (which developers are required to provide under Section 22756.3 of the proposed bill). Employers with fewer than 25 employees will not be required to perform this assessment, unless the automated system impacted more than 999 people in the calendar year.

NOTICE REQUIREMENTS

Employers using automated decision tools are required to notify any person subject to a consequential decision that the automated decision tool is being used to make a consequential decision. The notice is required to include: 1) a statement of the purpose of the automated decision tool; 2) contact information of the employer; and 3) a plain language description of the automated decision tool. If the consequential decision is made solely based on the output of the automated decision tool, the employer is required to, if technically feasible, accommodate a person's request to be subject to an alternative selection process.

GOVERNANCE PROGRAMS

Employers using automated decision tools are required to establish a governance program to address any reasonable foreseeable risks of algorithmic discrimination associated with the use of an automated decision tool. The governance program must, among other things, designate at least one employee responsible for overseeing and maintaining the governance program and compliance with AB 2930; implement safeguards to address reasonably foreseeable risks of algorithmic discrimination; conduct an annual and comprehensive review of policies, practices and procedures to ensure compliance with AB 2930; and maintain results of impact assessments for at least two years. Employers with fewer than 25 employees will not be required to form a governance program, unless the automated system impacted more than 999 people in the calendar year.

POLICY DISCLOSURE REQUIREMENTS

Any employers or developers using or developing automated decision tools are also required to make publicly available a clear policy that provides a summary of the types of automated decision tools currently in use and how the employer or developer manages the reasonably foreseeable risks of algorithmic discrimination that may arise from the use of the automated decision tools it uses.

LIABILITY FOR NON-COMPLIANCE

AB 2930 also provides mechanisms for penalizing non-compliance, including administrative fines up to $10,000 in administrative actions brought by the California Civil Rights Department and civil penalties through civil actions brought by district attorneys and city prosecutors.

Kevin J. White
Partner, Washington, DC and Houston

Jesse D. Borja
Associate, Los Angeles

INSURANCE

What Is Artificial Intelligence? Insurance Wants to Know

It is no secret that insurance stakeholders are waiting with bated breath to see how the insurance industry will address the risks and opportunities posed by artificial intelligence (AI). As stakeholders consider various insurance products and their coverage for AI risks, the definition of AI is vital. The reason is that if the bounds of AI are not delineated, then efforts to either grant or restrict insurance coverage for AI are likely to be futile.

As influential Enlightenment thinker John Locke explained long ago: "So difficult it is to show the various meanings and imperfections of words when we have nothing else but words to do it with." This statement has proved particularly prescient in the insurance field. Because insurance policies must, by their nature, reduce abstract and often complex concepts to writing, the various meanings and imperfections inherent in certain words have been, and will always be, a vexing issue for insurers and policyholders alike.

Examples of disputes about the meaning of specific words in the insurance field are wide-ranging. For example, does the word "automobile" include an 18-wheeler? Are jet-skis "watercrafts?" Does property sustain "physical loss or damage" when a harmful substance or virus changes the condition of the property such that it no longer functions as intended? Does the phrase "because of" mean any causal connection at all or is it limited to foreseeable causal relationships? Are there circumstances where the word "or" can actually mean "and" in context? The examples of word-choice are many, but the point is the same: without a stable, predictable and limited definition of a given term or phrase, disputes about the scope of insurance coverage are all but certain to arise with real-world consequences.

AI presents the latest frontier in this centuries-old definitional quest. On the one hand, the definitional problem is the same as with other words in that there is inherent difficulty in distilling abstract intellectual concepts in writing. On the other hand, AI poses new challenges due to its technological complexity and novelty. That is, there are at least seven forms of AI that presently exist or could exist and it is essential that insurance policy definitions adequately capture which is included and excluded. Compound this complexity with the reality that the average consumer of commercial insurance will have little understanding (if any) as to which forms of AI are being utilized in the insured business operations:

1. Reactive Machines AI: These are the simplest AI systems. They are purely reactive and can neither form memories nor use past experiences to inform current decisions. They are meant to perform specific tasks and their behavior is deterministic.
2. Limited Memory AI: These AI systems can learn from historical data to make decisions. They can store past experiences or data for a brief time. An example of this is self-driving cars that observe other cars' speed and direction.
3. Theory of Mind AI: This is a more advanced type of AI that can understand thoughts and emotions that affect human behavior. They can interact socially. This type of AI currently exists only in theory.
4. Self-Aware AI: This is the final stage of AI development which currently exists hypothetically. Self-aware AI, which currently exists only in theory and science fiction, would be systems that have their own consciousness and self-awareness.
5. Artificial Narrow Intelligence: Also known as Weak AI, this type of AI is meant to perform a narrow task, such as voice recognition. These systems can only learn or be taught how to do specific tasks.
6. Artificial General Intelligence: Also known as Strong AI, this type of AI refers to a system that possesses the ability to perform any intellectual task that a human can do. They can understand, learn, adapt and implement knowledge in a broad range of tasks.
7. Artificial Superintelligence: This refers to a time when the capability of computers will surpass humans. ASI is currently a hypothetical concept often depicted in science fiction. It is proposed to be capable of extraordinary cognitive capabilities, including the ability to understand and master any intellectual task that a human can do.

Considering these AI variants, the question for insurance industry participants is how to achieve contractual certainty while maintaining reasonable scope. The answer to this question can have wide-ranging, multi-billion-dollar implications.

Apart from the inclusion or exclusion of certain categories of AI, the definition of AI ultimately used in insurance policies will have to grapple with technologies or business processes that only use AI as a single subcomponent. In other words, insurance policy terms will have to be drafted to account for AI-enabled or AI-adjacent technologies—not technologies that solely use AI.

In sum, it remains to be seen how insurers will define AI in new policy forms. But as definitions are formulated and proposed, it is important to consider all definitional angles so that all involved parties can have as much certainty as possible about insurance products being bought or sold.

Michael S. Levine
Partner, Washington, DC and New York

Alex D. Pappas
Associate, Washington, DC

PRIVACY AND CYBERSECURITY

The Latest Developments in AI Legislation in Europe and the U.S.

In recent months, significant advances in AI legislation and governance have been made in Europe and the U.S., with far-reaching implications for privacy and cybersecurity. The European Parliament adopted the highly anticipated Artificial Intelligence Act (AI Act), introducing comprehensive rules governing the use of AI in the EU.

Shortly later, in the United States, the National Telecommunications and Information Administration (NTIA) issued its AI Accountability Report, while the Office of Budget and Management (OMB) released policy guidance to federal agencies on AI risk-management practices. These reports and guidance were published in the wake of President Biden's Executive Order (EO) on AI, issued last October. The OMB policy represents one such action at the 150-day mark of the EO.

AI Regulation in the EU: Scope of the EU AI Act
On March 13, 2024, the European Parliament formally adopted the AI Act. The AI Act is expected to take effect between May and June 2024. It is, therefore, important that businesses developing or using AI start assessing whether such AI systems fall within the scope of the AI Act. The scope of the AI Act has three key elements: (i) capacity of a business, (ii) geographical scope, and (iii) nature of the AI system.

The AI Act envisages four capacities within which a business can engage with AI, specifically:

1. Provider: a business that develops an AI system or a general purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark.

2. Deployer: a business using an AI system under its authority (except where the AI system is used in the course of a personal non-professional activity).
3. Importer: a business located or established in the EU that places on the market an AI system that bears the name or trademark of a business established outside the European Union (EU).
4. Distributor: a business in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.

Of the four capacities, the provider is subject to the most stringent obligations under the AI Act.

The AI Act applies to businesses acting in one or more of the above capacities located or established both within and outside the EU; i.e., the AI Act has extra-territorial scope, like other EU regulations. In this respect, the AI Act applies to:

- providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of their location or establishment;
- deployers of AI systems that have their place of establishment or are located within the EU;
- providers and deployers of AI systems that have their place of establishment or are located outside the EU, where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems;
- product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; and
- authorized representatives of providers which are not established in the EU.

THE NATURE OF THE AI SYSTEM

The AI Act introduces a risk-based legal framework that establishes different requirements depending on the level and type of risks related to the use of the concerned AI system. The AI Act establishes the following types of AI systems: (i) prohibited AI systems, (ii) high-risk AI systems, (iii) systems with transparency requirements, and (iv) general-purpose AI models. The different types of AI systems listed below are not mutually exclusive. For example, a high-risk system may also be subject to transparency requirements.

Prohibited AI Systems

Prohibited AI systems are AI systems and/or uses of AI that are deemed unacceptable from a fundamental rights perspective and, therefore, are prohibited. Examples of these include:

- AI systems that use subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques and that aim at or result in materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to make a decision that that person would not have otherwise made in a manner that causes or is likely to cause that person, another person or group of persons significant harm.
- AI systems that exploit a person's or a specific group of persons' vulnerabilities due to their age, disability or a specific social or economic situation and that aim at or result in materially distorting the behavior of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm.
- AI systems used to evaluate or classify natural persons or groups of persons over a certain period of time based on their social behavior or known, inferred or predicted personal or personality characteristics.
- AI systems used to infer emotions of a natural person in the areas of workplace and education institutions.
- Biometric categorization systems that categorize individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

High-Risk Systems

High-risk AI systems are deemed to present a potentially high-risk to the rights and freedoms of individuals. The AI Act differentiates two buckets of high-risk AI systems:

1. An AI system will be considered high-risk when: (i) it is intended to be used as a safety component of a product, or the AI system is itself a product covered by the EU harmonization legislation identified in Annex I of the AI Act and (ii) the product or system has to undergo a third-party conformity assessment under applicable EU harmonization legislation. This may cover AI systems used in, among others, machinery, toys, lifts, equipment and safety components for use in medical devices and in vitro diagnostic medical devices, civil aviation related products, marine equipment, rail system related products and various types of vehicles.

2. Annex III of the AI Act lists AI systems that are considered as high-risk directly by the AI Act itself, except if those systems do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons. High-risk AI systems identified in Annex III are divided in eight categories, examples of which include:
   - **Biometrics,** including remote biometric identification systems and emotion recognition AI systems.
   - **Critical infrastructure,** including AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity.
   - **Education and vocational training,** including AI systems intended to be used to determine the access, admission or assignment to educational and vocational training institutions at all levels.
   - **Employment, workers management and access to self-employment,** including AI systems intended to be used to recruit or select individuals, in particular to place targeted job advertisements, to analyze and filter job applications and to evaluate candidates.
   - **Access to and enjoyment of essential private services and essential public services and benefits,** including AI systems intended to be used to evaluate the creditworthiness of individuals or establish their credit score (except for AI systems used to detect financial fraud and risk assessment), or to be used for pricing in relation to individuals in the case of life and health insurance.

AI Systems With Transparency Requirements

AI systems with transparency requirements are deemed to pose specific transparency risks or to potentially mislead end-users due to their nature. Examples of these include:

- AI systems intended to interact directly with individuals;
- AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content;
- AI systems that generate or manipulate image, audio or video content constituting a deep fake; and
- AI systems that generate or manipulate text which is published with the purpose of informing the public on matters of public interest.

The form of transparency required will differ depending on the AI system and may include, for example, a label, notice or pop-up.

General-Purpose AI Models

A general-purpose AI model is an AI model, trained with a large amount of data using self-supervision at scale, which displays significant generality and is capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications, including serving as a basis for general purpose AI systems.

In addition, the AI Act also establishes the category of general purpose AI models with systemic risk for the more advanced general purpose AI models, to be designated by the European Commission. General purpose AI models with systemic risk will be subject to additional obligations regarding model evaluation and testing, risk mitigation, security and incident reporting.

While the AI Act is expected to take effect between May and June 2024, the provisions will take effect on a progressive basis between 6 and 36 months. Businesses should use this time to identify what AI systems they are engaging with in order to be able to determine whether such engagement is subject to the AI Act. From there, a business can then seek to map out how it will comply with the relevant provisions of the AI Act, leveraging relevant existing policies, procedures and measures where appropriate.

Federal AI Guidance in the United States

On March 27 and 28, 2024, the NTIA issued its AI Accountability Report, and the OMB issued a government-wide memorandum detailing AI risk-management practices. While this guidance is not legally binding on the private sector, it nonetheless sets standards and impacts the AI marketplace.

NTIA AI ACCOUNTABILITY REPORT

On March 27, 2024, the NTIA issued its AI Accountability Report.

The NTIA's AI Accountability Report, for which the NTIA published a Request for Comment (RFC) in April 2023, focuses on the idea that AI accountability policies and mechanisms are critical to optimizing AI technology. In particular, evaluation of AI systems, both pre- and post-release, and transparency around AI systems is necessary for innovation and adoption of trustworthy AI and for fostering stakeholder trust. The report details recommendations around the following aspects of the "AI accountability chain":

- Access to information: disclosures, documentation, access;
- Independent evaluation: evaluations, audits, red teaming; and
- Consequences for responsible parties: liability, regulation and market.

Based on stakeholder meetings, and the more than 1,400 comments received in response to its RFC, the NTIA developed eight major policy recommendations related to the AI accountability chain under the categories of Guidance, Support and Regulatory Requirements.

Guidance

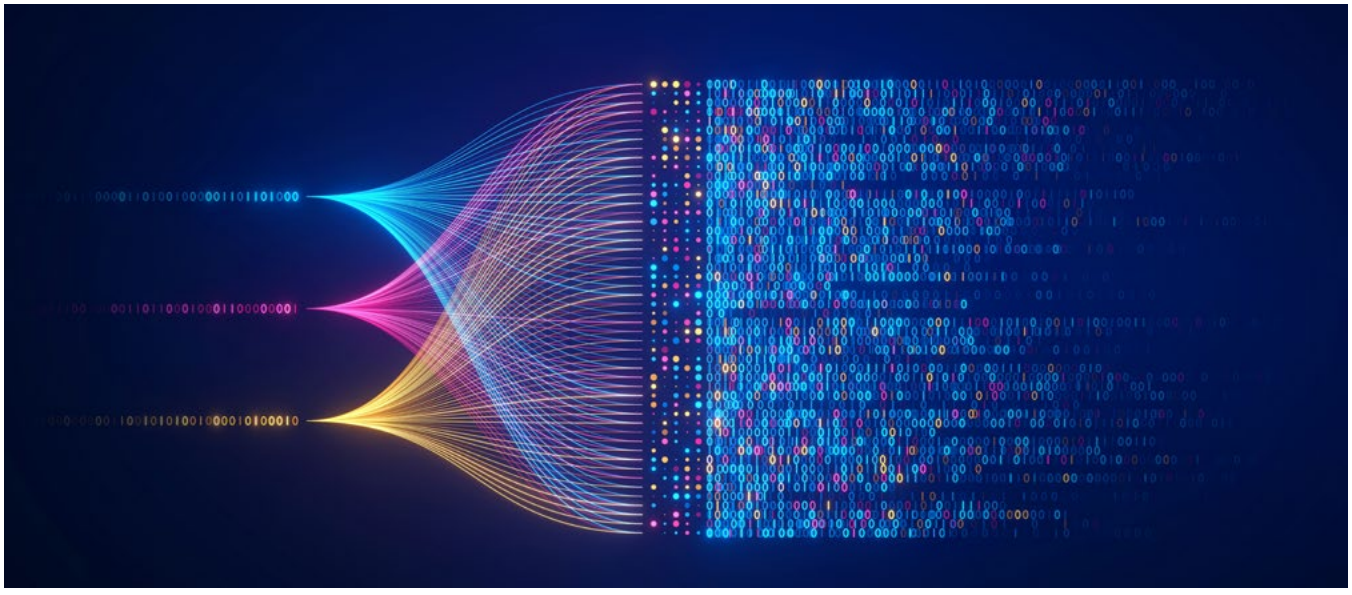
The NTIA recommends that federal agencies work with stakeholders to create basic guidelines for AI audits and auditors, and suggests the creation of auditor certifications and audit methodologies. The report also suggests that the federal government work with stakeholders to improve standard information disclosures, so that they are accessible to their respective audience, including impacted people, developers or regulators. As the report suggests, one disclosure method could include the use of nutritional labels for AI systems, similar to standard food nutrition labels. Lastly, the report calls for regulatory agencies to clarify how existing laws and regulations apply to AI systems with respect to liability.

Support

The report recommends that federal agencies invest in the necessary resources to support the independent evaluation of AI systems, including by creating the National AI Research Resource (NAIRR). Further, the report calls for federal agencies to support the development of AI testing and evaluation, including the development of tools that facilitate access to AI system components for evaluators and researchers, while maintaining data privacy and security.

Regulatory Requirements

The NTIA also recommends that federal agencies require independent audits of high-risk AI models, and suggests the government take steps to bolster its capacity to address cross-sector AI risks such as by maintaining a national registry of high-risk AI deployments. Further, the report notes that the federal government's purchasing power allows it to influence standards in the AI marketplace, and advises the government to require its suppliers and contractors to adopt federally recognized AI standards and risk management practices.



OMB AI RISK MANAGEMENT POLICY

On March 28, 2024, the White House announced the Office of Budget and Management's (OMB's) first government-wide policy on AI risk management.

The OMB Policy to Advance Governance, Innovation and Risk Management in Federal Agencies' Use of Artificial Intelligence, announced by Vice President Kamala Harris, is a "core component" of the EO on AI, provides the basis for multiple areas of AI accountability and governance, and will be foundational for other agencies to build upon in developing subsequent regulations, many of which will in turn impact the private sector. The OMB Policy was issued as a memorandum directing heads of federal agencies to implement practices such as:

- addressing risks related to the use of AI (e.g., mandatory assessments and safeguards);
- expanding transparency of AI (e.g., reporting AI use cases and metrics);
- advancing responsible AI innovation for high priority societal challenges (e.g., climate change, public health, public safety);
- growing the AI workforce (e.g., hiring AI professionals and setting pay and leave guidance); and
- strengthening AI governance (e.g., designating chief AI officers and establishing AI governance boards).

The White House also announced several of its upcoming actions, including a request for information (RFI) for responsible AI procurement, expanding the government's AI Use Case Inventory and hiring 100 AI professionals by summer 2024.

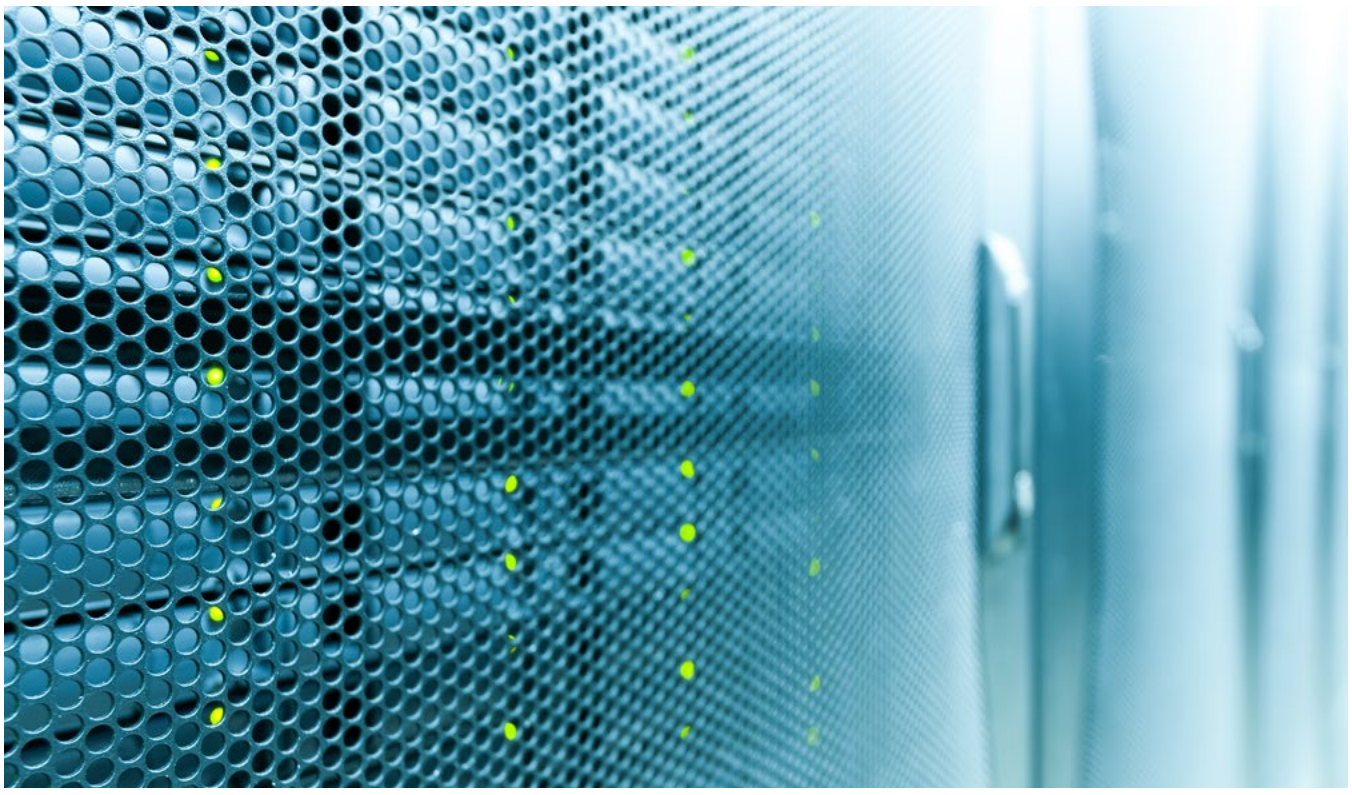
These types of policies and reports are anticipated to inform compliance efforts in the rapidly evolving AI environment, including in the privacy and security arenas.

Sarah Pearce
Partner, London

Jennie Cunningham
Associate, New York

Tiago Sérgio Cabral
Associate, Brussels

Liliana Fiorenti
Law Clerk, New York



CORPORATE

AI Washing: The SEC Is Focused on Your AI Disclosures

The pace of SEC rulemaking has been fast and furious recently and its focus on emerging technology and cybersecurity is sharper than ever. In addition to the SEC's increased enforcement activity in the digital asset space and new disclosure rules related to cybersecurity risks, they have also become increasingly focused on AI washing, both in enforcement actions and public remarks. "AI washing" (which follows the trendy ESG-related term, "Greenwashing") is the new buzzword to describe a company overexaggerating its use of AI in an attempt to attract investors.

Recent SEC Enforcement Actions Targeting AI Washing

In March, the SEC announced the settlement of enforcement actions against two different investment advisers, both of which were charged with making false and misleading statements about their purported use of AI. Civil penalties in these settlements were collectively $400,000.

In one case, the SEC targeted statements made on the firm's marketing materials, press releases and website that claimed, for example, that the firm "[p]uts collective data to work to make our artificial intelligence smarter so it can predict which companies and trends are about to make it big and invest in them before everyone else." The SEC found that this and related statements about the firm's use of AI were false or materially misleading after the firm admitted during the investigation that, "it had not used any of its clients' data and had not created an algorithm to use client data."

In the other case, the SEC found that the firm made false and misleading statements on its website and social media about its purported use of AI. For example, the firm falsely claimed to be the "first regulated AI financial advisor" and falsely claimed that its platform provided "[e]xpert AI-driven forecasts."

The SEC's message is clear with these enforcement actions, if you say you are using AI, you better be sure that you are. In a video released about these enforcement actions, the SEC's Director of the Division of Enforcement, Gurbir S. Grewal said that these, "enforcement actions should serve notice to the investment industry, that if you claim to use AI in your investment processes, you must ensure that your representations aren't false, they aren't misleading."

SEC's Public Warnings Against AI Washing

In a speech in February, SEC Chair Gary Gensler had AI top of mind and focused almost the entirety of his remarks on AI and the SEC's corresponding regulatory duties. Chair Gensler was first focused on the risks he sees associated with the use of AI including, the conflicts of interests raised by AI for advisers, the problems presented by AI hallucinations and the threat that AI could pose to the stability of capital markets. According to Chair Gensler, AI washing encompasses not just outright false claims, but also overly generalized disclosures that do not actually help investors. With AI making the headlines almost daily, companies may feel pressured to reference AI in some way in their public disclosures, even if there is not anything concrete to report. This, Chair Gensler says, is a mistake. In particular, he cautioned against:

- boilerplate AI disclosures not particularized to the company;
- disclosing the use of AI models when the underlying technology is not actually AI-driven; and
- AI-related projections that do not have a reasonable basis.

In March, on the same day that the SEC announced the AI washing settlements discussed above, Chair Gensler released one of his infamous YouTube videos focused entirely on AI washing. In the video, while acknowledging that "AI is the most transformative technology of our time," he expresses his concern that, "when new technologies come along, we've also seen time and again false claims to investors by those purporting to use those new technologies." In no uncertain terms, Chair Gensler makes clear "that AI washing may violate the securities laws."

Chair Gensler has been joined in his warnings to the public markets by the SEC's Director of the Division of Enforcement, Gurbir S. Grewal. In public remarks in April, Director Grewal focused on his perceived problematic disclosures by investment firms on their use of AI as well as disclosures by public companies. Director Grewal cautioned investment firms to pause before making claims about their use of AI in the investment process to attract new investors.

> 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.

Director Grewal also encouraged "proactive compliance" as a tool to avoid violating disclosures rules when it comes to AI washing, suggesting that companies and their counsel should focus "education, engagement, and execution."

- Individuals responsible for a company's disclosures should first educate themselves on emerging and heightened AI risks by reviewing the SEC's enforcement actions, reading Chair Gensler's remarks on AI, staying updated on how AI-related issues are actually impacting companies in practice.
- After educating themselves, individuals responsible for public disclosure should engage stakeholders inside their company's different business units to learn how AI intersects with their activities, strategies, risks, financial incentives, etc.
- Finally, companies should then execute a plan to ensure their internal policies, procedures and disclosure controls appropriately reflect how the company is actually using AI and the related risks.

Takeaways

If you are a public company that is either using AI, thinking about using AI or in an industry that AI has the potential to impact, now is the time to critically think about your public disclosures. It is a public company's responsibility to be able to articulate to investors how the company is using AI without crossing the line into aspirational uses that are not yet viable or deployed. At the same time, the risks of using, or not using AI, must also be analyzed and disclosed to the extent material to the business. For example, saying nothing about AI if your company is exposed to AI-related risks is also potentially a problem.

As we have seen with other emerging technologies, it is more important than ever for the legal department to be working closely with product and strategy teams to really understand how a company is using AI. If the risks of AI washing are properly managed, how a company describes its use of AI and the related risks presents an opportunity to successful engage with investors in the space.

Mayme Beth F. Donohue
Partner, Richmond

Alexander Abramenko
Associate, Washington, DC

HUNTON ANDREWS KURTH