

THE Procurement LAWYER



AMERICAN BAR ASSOCIATION
Public Contract Law Section

SECTION OF PUBLIC CONTRACT LAW
AMERICAN BAR ASSOCIATION
VOLUME 59, NUMBER 4
SUMMER 2024

What Government Contractors Need to Know About Artificial Intelligence Legal Issues

BY JAMES GATTO AND TOWNSEND BOURNE



James Gatto



Townsend Bourne

The rapid growth of artificial intelligence (AI) adoption creates opportunities for government contractors. In particular, the US government's desire to increase its use of AI in government systems means contractors can help build out those systems. And like other companies, contractors can leverage AI to operate their own businesses

Jim Gatto is a partner in the Intellectual Property Practice Group in Sheppard Mullin's Washington, DC, office. He is co-leader of the Artificial Intelligence Team and Blockchain & Fintech Team and leader of the Open Source Team. For over 35 years, he has been a thought leader on legal issues with emerging technologies and business models, most recently blockchain, AI, open source, and interactive entertainment. He provides strategic advice on all aspects of intellectual property strategy and enforcement, technology transactions, licenses, and tech-related regulatory issues (e.g., securities, gambling, and AML), especially ones driven by new business models and/or disruptive technologies. Townsend Bourne is a partner in the Governmental Practice in Sheppard Mullin's Washington, DC, office. She is leader of the firm's Government Business Group and the Governmental Practice Cybersecurity & Data Protection Team. Townsend is a strategic thinker and advocate for companies that do business with the US government, either directly or through a prime contractor or reseller. She specializes in counseling clients on issues involving cybersecurity, supply chain risk management, critical infrastructure, and emerging technologies, including FedRAMP, AI, and incident response.

more efficiently. But as government contractors seize these AI opportunities, they must grapple with a range of new legal issues as well.

The federal government has been grappling with similar issues, and particularly with how to regulate and procure this rapidly evolving technology. In October 2023, the Biden administration released Executive Order 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," establishing the White House's position on key aspects related to the use of AI.¹ Additionally, various agency initiatives are underway, as a result of both the Executive Order and otherwise, to influence use of AI going forward. Notably, Executive Order 14110 mandated 150 specific actions for various government agencies to implement within very aggressive timelines. Agencies timely completed these action items,² which is truly a feat in the government world and signals the dedication and importance being placed on AI issues.

One key area, to which many of the mandates relate, is "responsible AI use." Companies that want to provide AI to the government will need to be aware of and adhere to these responsible AI use principles. Companies

continued on page 21

ISSUE HIGHLIGHTS

News from the Chair	2
CMMC Cybersecurity Proposed Rule	3
The Federal Circuit's "Jurisdictional Triumvirate"	11
News from the Committees	17
Summary of PCL Spring Committee Showcase Event	19
In Memoriam: George M. "Tim" Coburn	32

ARTIFICIAL INTELLIGENCE LEGAL ISSUES

continued from page 1

that use AI in their operations must be aware of and develop AI use policies based on these principles, as well as a host of other legal issues. And if companies are using third-party AI tools, they need to ensure they conduct AI-specific vendor diligence.

This article describes key federal government initiatives relating to artificial intelligence and important considerations for government contractors on the use and development of AI. This article includes an overview of key legal issues, recommended elements of corporate AI policies, and important issues to consider when conducting AI-specific vendor diligence for contractors (and all companies, for that matter).

US Government AI Policy and Initiatives

Background on US Government AI Policy

Leading up to the release of Executive Order 14110, the White House in October 2022 published its “Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People.”³ This document outlines five principles focused on ensuring protections for Americans with respect to AI: (1) Safe and Effective Systems, (2) Algorithmic Discrimination Protections, (3) Data Privacy, (4) Notice and Explanation, and (5) Human Alternatives, Consideration, and Fallback. The AI Bill of Rights is a voluntary, nonbinding framework that forms the basis for protections that were eventually included in Executive Order 14110.

In 2023, the federal government engaged in additional efforts to define its approach to AI. On January 23, 2023, the National Institute of Standards and Technology (NIST) released the first version of its “Artificial Intelligence Risk Management Framework” (AI RMF).⁴ This framework is a resource for organizations designing, developing, deploying, or using AI systems regarding management of risks associated with AI and promoting trustworthy and responsible development and use of AI systems. The NIST AI RMF is a voluntary framework.

On April 20, 2023, the Secretary of Homeland Security announced a new initiative to combat evolving threats, including those related to generative AI.⁵ The initiative includes the creation of an AI Task Force that will drive specific AI applications to advance critical homeland security missions, including (1) integrating AI to enhance the integrity of supply chains and the broader trade environment, such as deploying AI to improve screening of cargo and identifying the importation of goods produced with forced labor, and (2) collaborating with government, industry, and academia partners to assess the impact of AI on the Department of Homeland Security (DHS)’s ability to secure critical infrastructure.

Further, on April 25, 2023, officials from the Federal Trade Commission (FTC), the Department of

THANK YOU TO OUR 2024 ANNUAL MEETING SPONSORS



SECTION LUNCHEON SPONSORS

Crowell & Moring LLP

Fried Frank Harris Shriver & Jacobson LLP

Haynes & Boone LLP

HKA Global, Inc.

K&L Gates LLP

Stinson LLP

Thompson Coburn LLP

Justice (DOJ), the Consumer Financial Protection Bureau (CFPB), and the US Equal Employment Opportunity Commission (EEOC) released a joint statement on “Enforcement Efforts Against Discrimination and Bias in Automated Systems.”⁶ And in July 2023 the White House met with and secured voluntary commitments from leading AI companies to manage the risks posed by AI.⁷ These commitments included (1) ensuring products are safe before being introduced to the public, (2) putting security first, and (3) working to earn public trust by ensuring transparency and accountability with respect to AI systems.

Executive Order 14110

Executive Order 14110 establishes a comprehensive framework for the development, deployment, and regulation of AI technologies.⁸ It underscores the importance of AI in enhancing national security, economic prosperity, and the quality of life of US citizens.⁹ Key sections of the Executive Order focus on (1) ensuring

safety and security of AI technology; (2) promoting innovation and competition; (3) supporting workers; (4) advancing equity and civil rights; (5) protecting consumers, patients, passengers, and students; (6) protecting privacy; (7) advancing federal government use of AI; and (8) strengthening American leadership abroad.¹⁰ The directive mandates federal agencies to prioritize AI in their budgets, encourages the private sector's investment in AI research and development, and emphasizes the need for international collaboration to establish global norms and standards for AI.¹¹

The anticipated effects of the Executive Order are far reaching and touch multiple industries and sectors. Most significant for companies and government contractors are the following actions stemming from the Executive Order. The Executive Order:

- Imposes testing obligations on developers of the most powerful systems and requires sharing results using the government's authority under the Defense Production Act;¹²
- Directs many agencies to take specific actions to protect consumers, patients, students, and workers;
- Contemplates assessments of job displacement due to AI, as well as potential remedies;
- Mandates efforts for managing content authentication and provenance (e.g., to prevent deepfakes);
- Calls on Congress to implement federal privacy legislation;
- Takes aim at "BAD" AI (biased and discriminatory AI) to promote equity and civil rights;
- Focuses on the government's responsible use of AI;
- Creates programs and provides resources to enhance US leadership in innovation;
- Promotes US leadership in coordinating global regulatory efforts; and
- Takes steps to protect US infrastructure from foreign bad actors' use of AI.¹³

In short, the federal government plans to leverage the positive aspects of AI but acknowledges the development, deployment, and use of AI must be done responsibly.

The Executive Order includes myriad tasks for agencies, with many due dates within 90 or 270 days of issuance of the Order.¹⁴ On January 29, 2024, the White House released a report announcing that agencies had completed all the 90-day action tasks by the Executive Order;¹⁵ and on April 29, 2024, the White House released a similar report announcing completion of all 180-day actions.¹⁶ Below we discuss those actions and initiatives that are key for companies that do business with the federal government, in addition to those in critical infrastructure sectors and other relevant industries.

NIST Guidelines and Best Practices

As noted above, NIST released its AI RMF prior to

issuance of Executive Order 14110. Under the Executive Order, NIST is further tasked with establishing guidelines, standards, and best practices relating to AI (building on its AI RMF).¹⁷ These new guidelines include (1) an AI RMF companion publication for generative AI; (2) a resource for secure software development practices for generative AI; (3) benchmarks for evaluating AI capabilities focusing on harm in cybersecurity and biosecurity; and (4) resources for development and testing to enable safe, secure, and trustworthy AI—particularly with regard to dual-use foundation models.¹⁸

As of the Executive Order's six-month mark, NIST released these new guidelines as draft documents for public comment. The documents include:

- AI RMF Generative AI Profile (NIST AI 600-1);¹⁹
- Secure Software Development Practices for Generative AI and Dual-Use Foundation Models (NIST Special Publication 800-218A);²⁰
- Reducing Risks Posed by Synthetic Content (NIST AI 100-4);²¹ and
- A Plan for Global Engagement on AI Standards (NIST AI 100-5).²²

NIST further announced its NIST GenAI program, which will evaluate generative AI capabilities through testing and seeks to tackle issues associated with identification of synthetic content.²³

The NIST guidance consists of voluntary frameworks to assist companies with the responsible development of AI. It does not have the force of law, but it may not be without legal significance. As in the cybersecurity space, where NIST standards form the basis for Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) requirements for security controls for sensitive information, NIST guidelines on AI are likely to be included in eventual laws and regulations applicable to companies and contractors that sell AI products and services to the federal government.

Additionally, based on some proposed state legislation, it is likely that adherence to the NIST AI RMF may be required sooner rather than later. For example, proposed Colorado state legislation seeks to impose obligations on developers and deployers of AI systems and provides an affirmative defense if they have implemented and maintained a program that complies with a nationally or internationally recognized risk management framework for AI systems.²⁴ NIST's AI RMF is one the most frequently cited risk management frameworks in the United States.²⁵

Critical Infrastructure

The 16 critical infrastructure sectors also are a focus of Executive Order 14110.²⁶ Per the Executive Order, relevant heads of agencies with authority over critical infrastructure will work with the Cybersecurity Infrastructure and Security Agency (CISA) to evaluate potential

risks related to the use of AI.²⁷ The Department of Commerce (DOC) and DHS are expected to incorporate the NIST AI RMF and other appropriate security guidance into relevant safety and security guidelines for critical infrastructure, in addition to expected regulatory actions that will likely mandate guidelines for critical infrastructure.²⁸ Further, DHS is tasked with establishing an AI Safety and Security Board with experts from the private sector, academia, and government to advise critical infrastructure on AI use.²⁹

As of the Executive Order's six-month mark, the federal government launched the "AI Safety and Security Board" to advise on responsible development and use of AI with respect to critical infrastructure.³⁰ Further, CISA released AI safety and security guidelines for critical infrastructure, which advises entities in critical infrastructure sectors to use the NIST AI RMF to manage use of AI and assess AI vendors and use cases.³¹ CISA also released its "Roadmap for Artificial Intelligence" in November 2023.³² Additionally, while not an initiative under the Executive Order, CISA separately released a proposed rule in April 2024 pursuant to the Cybersecurity Incident Reporting & Critical Infrastructure Act (CIRCA) that will require covered entities in each of the critical infrastructure sectors to report substantial cyber incidents to CISA within 72 hours and ransom payments within 24 hours.³³

Software Security and Vulnerabilities

The Department of Defense (DoD) is working on a pilot program for new AI tools to identify and address software vulnerabilities—specifically relating to the military and national security.³⁴ DHS similarly is engaged in efforts to combat software vulnerabilities in key software systems.³⁵ Ensuring secure software development was a key focus of another Executive Order (E.O. 14028, Improving the Nation's Cybersecurity).³⁶ As of June 2024, the FAR Council is working on a proposed rule that will require producers of software purchased and used by the federal government to attest to compliance with secure software development practices developed by NIST (NIST SP 800-218).³⁷ CISA has released a common attestation form for software producers related to secure software development.³⁸

Guidance Relating to Workers

A focus of Executive Order 14110 is ensuring AI is deployed in ways that can complement and empower workers, and that issues associated with worker displacement are fully considered. As of the Executive Order's six-month mark, the Department of Labor had developed two key resources. The first is an Office of Federal Contract Compliance Programs (OFCCP) guide specifically for federal contractors and subcontractors addressing legal issues, equal employment opportunity obligations, and how to mitigate potential negative effects such as discrimination associated with use of AI relating

to hiring and employment decisions.³⁹ The second is guidance relating to the use of AI as it relates to obligations under the Fair Labor Standards Act and other federal labor standards.⁴⁰ Similarly, the Office of Personnel Management (OPM) released guidance for federal workers on use of generative AI tools, which can be used to inform contractor AI use policies and procedures.⁴¹

Synthetic Content

Synthetic content (i.e., computer-generated data that mimic and are easily mistaken for real-world data) is a concern addressed in Executive Order 14110, particularly where such content subjects Americans to AI-enabled fraud and deception (including deepfakes). The

A focus of Executive Order 14110 is ensuring AI is deployed in ways that can complement and empower workers, and that issues associated with worker displacement are fully considered.

Executive Order seeks to protect Americans by instituting measures to establish the authenticity and provenance of digital content, both synthetic and not synthetic, produced by the federal government or on its behalf.⁴² It also suggests agency actions to foster capabilities for identifying and labeling synthetic content, such as use of watermarking and clear labeling of AI-generated content.⁴³ Importantly, the only mention of potential updates to the FAR in the Executive Order relates to synthetic content—the Executive Order states the FAR Council should "consider" updating the FAR to incorporate guidance on synthetic content.⁴⁴

As one part of its response to the Executive Order mandates, NIST published *Reducing Risks Posed by Synthetic Content* (NIST AI 100-4).⁴⁵ This publication provides technical approaches for promoting transparency in digital content based on use case and context. This publication identifies methods for detecting, authenticating, and labeling synthetic content, including digital watermarking and metadata recording, where information indicating the origin or history of content such as an image or sound recording is embedded in the content to assist in verifying its authenticity. This

publication supplements a separate report on provenance and detection of synthetic content that Executive Order 14110 Section 4.5(a) tasks NIST with providing to the White House.

The report offers approaches to help manage and reduce risks related to synthetic content in four ways:

- Attesting that a particular AI system produced a piece of content;
- Asserting ownership of content;
- Providing tools to label and identify AI-generated content; and
- Mitigating the production and dissemination of AI-generated child sexual abuse material and non-consensual intimate imagery of real individuals.

As this is the one topic on which the Executive Order mentions the FAR Council, contractors should take note and ensure they are appropriately identifying and managing synthetic content.

Infrastructure as a Service (IaaS) Providers

Concerns over foreign malicious cyber actors and the use of US Infrastructure-as-a-Service (IaaS) providers led the Biden administration to mandate new regulations in this space. The Department of Commerce released proposed regulations for IaaS providers to report transactions with foreign persons to train large AI models with potential malicious cyber capabilities and to develop Know Your Customer programs to verify the identity of foreign customers and ensure foreign resellers of US IaaS products verify the identity of any foreign person that obtains an IaaS account from the foreign reseller.⁴⁶ Comments on the proposed regulations will be reviewed and the Department of Commerce will issue a final rule.

National Security Memorandum

Executive Order 14110 calls for development of a National Security Memorandum on AI for the president within 270 days (by July 26, 2024). This will address the governance of AI used as a component of a national security system or for military or intelligence purposes and provide guidance to DoD, other relevant agencies, and the Intelligence Community regarding the continued adoption of AI capabilities to advance national security missions. In addition, the Executive Order calls for continued actions for addressing the potential use of AI systems by adversaries and foreign actors that threaten DoD or Intelligence Community capabilities/objectives, or otherwise pose a risk to the security of the United States and its partners and allies.

Ensuring Responsible AI Use by the US Government

A key aspect of Executive Order 14110 includes examining how the US government itself plans to use AI technologies internally and institute appropriate

procurement procedures for AI technologies. The government is focused on actions to ensure responsible deployment of AI by the government and the modernization of federal AI infrastructure. The Executive Order calls for an interagency council to coordinate development and use of AI in government programs and operations. Further, the Office of Management and Budget (OMB) recently finalized its memorandum for agencies that will form the basis for its actions on AI going forward. On March 28, 2024, OMB issued Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*.⁴⁷ This is the final version of a draft memorandum OMB released originally on November 1, 2023.⁴⁸ The memorandum focuses on responsible development, testing, and operation of AI by the federal government, as well as managing risks in federal procurement of AI.

Per the memorandum, agencies must designate a Chief AI Officer responsible for coordinating agency use of AI and promoting AI innovation, while also managing the risks associated with the use of AI. Further, agencies are to release publicly on their websites their strategy for removing barriers to the responsible use of AI. Although the memorandum emphasizes collaboration and sharing between agencies of AI code, models, and data, this is subject to applicable law, contractual obligations, and national security risks.

The memorandum also outlines minimum practices applicable to new and existing AI developed, used, or procured by or on behalf of agencies for “Safety-Impacting AI”⁴⁹ and “Rights-Impacting AI.”⁵⁰ These minimum practices include (1) completing an AI impact assessment; (2) testing AI for performance in a real-world context; (3) independently evaluating and authorizing AI; (4) conducting ongoing monitoring; (5) regularly evaluating risks from AI; (6) mitigating emerging risks to rights and safety; (7) ensuring adequate human training and assessment; (8) providing additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety; and (9) providing public notice and plain-language documentation for AI use cases. The memorandum also includes certain exclusions from the minimum practices and additional minimum practices applicable to Rights-Impacting AI focused on equity, fairness, and mitigating algorithmic discrimination when it is present.

Federal Procurement of AI

With respect to federal procurement of AI, the OMB memorandum provides recommendations to agencies for responsible purchasing of AI as well as promoting competition and ensuring the government retains sufficient data rights and computer software rights in the design, development, testing, and operation of the AI. The following are recommendations for managing risks in federal procurement of AI:⁵¹

- **Aligning with the Law:** Procurement of AI should be consistent with applicable laws, regulations, and policies, with a particular emphasis on addressing privacy, confidentiality, intellectual property (IP), cybersecurity, human and civil rights, and civil liberties.
- **Transparency and Performance Improvement:** Agencies should seek adequate documentation regarding the procured AI's capabilities and known limitations and the provenance of the data used to train and operate the AI. There should be continuous monitoring post-award to mitigate risk and incentivize improvement of the procured AI.
- **Promoting Competition in Procurement of AI:** Agencies should promote interoperability of procured AI to ensure the government does not improperly entrench incumbents or permit vendors to favor their own products.
- **Maximizing the Value of Data for AI:** Agencies are encouraged to include contractual provisions to retain software rights and rights to data, as well as any improvements to the data to ensure the agency's continued design, development, testing, and operation of AI. (This will be a key area for contractors' focus to ensure software and data rights align with expectations.) Agencies also will consider including contract provisions regarding protection of federal information used by vendors in the development and operation of AI products and services for the government, including protection from unauthorized disclosure and prohibiting vendors from subsequently using the software or data to train or improve the functionality of the vendor's commercial offerings without express permission from the agency.
- **Overfitting to Known Test Data:** Agencies should act appropriately to ensure AI developers or vendors are not directly relying on test data to train their AI systems where this could result in the system appearing more accurate in tests than in real-world applications.
- **Assessing for Environmental Efficiency and Sustainability:** Agencies are encouraged to consider the environmental impact of computationally intensive AI services (e.g., those reliant on dual-use foundation models), including methods to improve efficiency and sustainability of AI.
- **Responsible Procurement of AI for Biometric Identification:** The OMB memorandum encourages agencies to take special care when procuring AI for biometric identification. This includes assessing and addressing risks that the data used may not be lawfully collected or used without appropriate consent or embed unwanted bias, or were collected without validation of the included identities.
- **Responsibly Procuring Generative AI:** When procuring generative AI tools, particularly dual-use

foundational models, the OMB memorandum encourages agencies to require adequate testing and safeguards and to require appropriate labeling of content generated or modified by AI. Agencies also are encouraged to incorporate relevant NIST standards such as the AI RMF and AI Risk Management Framework for Generative AI.

Various agencies, including the General Services Administration (GSA), have announced AI prioritization initiatives and plans for more funding for AI projects.

At the end of April 2024, GSA released its "Generative AI and Specialized Computing Infrastructure Acquisition Resource Guide."⁵² This guide is a high-level resource outlining potential uses of generative AI for government agencies and procurement strategies. Interestingly, the guide suggests agencies consider whether "no new acquisition" is an acceptable solution through use of Software-as-a-Service (SaaS) generative AI tools accessible through publicly available websites or use of generative AI tools offered by existing government cloud platform providers. To ensure competition requirements are followed and to limit potential protests, use of new generative AI tools under an existing cloud platform contract would need to be within the scope of the contract. While GSA does not plan for a separate Schedule contract for AI, many AI tools can be purchased under the existing Multiple Award Schedules (MAS) IT (MAS IT) or Government-Wide Acquisition Contracts (GWACs). In some cases, agencies may elect to seek custom AI solutions. This could be done through Cooperative Research and Development Agreements (CRADAs), Other Transaction Authority (OTA) agreements, or open-market buys, although GSA encourages the use of MAS IT or GWACs over open-market buys to mitigate financial and compliance risk.

It will be important for contractors in this space to stay up-to-date on government guidance and practices for managing the risks associated with the use of AI to be able to provide solutions that meet government requirements and ensure the safe and responsible design, development, and use of AI.

Security and FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's program for security authorizations for cloud service offerings for the government. Per Executive Order 14110, the FedRAMP Program Management Office is charged with developing a framework to prioritize emerging technologies in the authorization process, starting with generative AI.

On January 26, 2024, the FedRAMP Program Management Office released its draft Emerging Technology Prioritization Framework, which includes the first three generative AI capabilities selected for FedRAMP prioritization: (1) chat interfaces, (2) code generators, and (3) debugging tools.⁵³ The emerging technologies selected

for prioritization will have a reduced waiting time before the authorization process (i.e., they get to skip the line), but the authorization process itself will not be accelerated. The framework also contemplates continuous collaboration among FedRAMP stakeholders to nominate additional emerging technologies for FedRAMP to consider for prioritization.

Regulating AI and Enforcement

There are two main agencies that will likely lead the charge on AI enforcement: the Federal Trade Commission (FTC) and the Department of Justice (DOJ).

The FTC has been actively involved in regulating AI and its applications, with a focus on curbing potential harms to consumers and competition. Recently, the FTC has issued warnings, guidance, and policy statements and engaged in enforcement actions related to AI.⁵⁴ Key topic areas related to FTC activity are privacy, biometric privacy, and security; accuracy; fairness and nondiscrimination; transparency and explainability; safety and reliability; and advertising.

One key area of FTC concern relates to the data used to train AI models. The FTC recognizes that the foundation of any generative AI model is the underlying data and that developing generative AI typically requires exceptionally large datasets, especially in the pretraining step. From a competition perspective, the FTC has noted that pretraining or fine-tuning a model with deep expertise in specialized areas may require access to large amounts of data that are not widely available and would be difficult for a new player in the market to collect.

The FTC also has warned that just because a company possesses data does not mean it has a right to use those data to train AI models. This comes as a surprise to many companies. Sometimes these data are collected over many years, often long before a company thought to use it for training AI. The potential problem is that the privacy policies in effect when the data were collected may not have considered this use. The use of customer data in a manner that exceeds or otherwise is not permitted by the privacy policy in effect at the time the data were collected could be problematic. This has led to class action lawsuits and/or enforcement by the FTC. In some cases, the FTC has imposed a penalty known as “algorithmic disgorgement” to companies that use data to train AI models without proper authorization. This penalty is severe as it requires deletion of the data, the models, and the algorithms built with those data. This can be an incredibly costly result.⁵⁵

Some companies that recognize this dilemma have sought to modify their terms of use or privacy policies. While this seems to be a logical “fix,” the FTC has raised concerns with this as well. In recent guidance, “AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive,” the FTC warned: “It may be unfair or deceptive for a company to adopt more permissive data practices—for example, to start sharing

consumers’ data with third parties or using that data for AI training—and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy.”⁵⁶

The guidance further explains that the FTC believes that companies face a potential conflict of interest in that “they have powerful business incentives to turn the abundant flow of user data into more fuel for their AI products, but they also have existing commitments [e.g., privacy and data security policies] to protect their users’ privacy.”⁵⁷ The FTC notes that companies might be tempted to resolve this conflict by simply changing the terms (e.g., their privacy policy) surreptitiously so they are no longer restricted in the ways they can use their customers’ data. The FTC further warns that market participants should be on notice that any firm that reneges on its user privacy commitments risks running afoul of the law.⁵⁸ Simply put, according to the FTC guidance, a business that collects user data based on one set of privacy commitments cannot then unilaterally revoke those commitments after collecting users’ data.

The FTC guidance provides examples of FTC enforcements for these practices (see, e.g., Gateway Learning Corporation and 1Health.io)⁵⁹ and warns that it will continue to bring actions against companies that surreptitiously rewrite their terms/privacy policies to allow themselves free rein to use consumer data.⁶⁰

Another key area of FTC concern relates to advertising of AI tools. The FTC cautions companies not to exaggerate what their AI products can do. Additional FTC guidance notes AI tool performance claims can be deceptive if they lack scientific support or if they apply only to certain types of users or under certain conditions.⁶¹ It adds that claims that an AI product does something better than a non-AI product should not be made without adequate proof. It also advises companies to understand the reasonably foreseeable risks and impact of an AI product before putting it on the market. If something goes wrong, a company cannot just blame a third-party developer of the technology and disavow responsibility because that technology is a “black box” the company is not able to understand or did not know how to test.⁶² This is one of the reasons that competent AI vendor diligence is critical, as further addressed below.

If a company is developing AI tools, the list of FTC concerns goes even deeper. The FTC provides a roadmap of the issues of which AI developers should be aware in the July 13, 2023, civil investigative demand letter (CID) it issued to OpenAI.⁶³ The comprehensive set of questions reveals the range of topics in which the FTC is interested, as well as the issues companies should ensure they consider when developing AI. Some of the topics include how data to train AI are obtained and reviewed, how training and testing are done, how accuracy and transparency are achieved, how errors are managed, and the human involvement in these processes. The CID questions seek OpenAI’s written policies to address these

and other AI issues. It is apparent from this CID that the FTC is focused on the policies that companies develop and implement to ensure responsible AI development. This is just one reason AI policies are necessary.

DOJ also is acting in the AI space. As part of enforcement under its Disruptive Technology Strike Force, DOJ plans to focus on AI and will seek more severe sentences where misuse of AI is involved in the offense.

Important Considerations for Companies

Executive Order 14110 and resulting agency actions will have significant implications for companies developing or deploying AI. The issues that companies face will differ depending on whether they are developing or deploying AI, or both.

In all cases, companies must ensure proper AI governance. It is advisable that companies develop an AI governance body. This group needs to include the appropriate stakeholders given the nature of the company. It is worth noting that federal agencies have appointed or are in the process of appointing a Chief AI Officer, and companies may consider instituting a similar position with oversight and responsibility for AI.

It is critical that members of the governance body receive adequate training to understand the current AI-related legal and regulatory issues and the business ramifications for noncompliance. It is also important that a process is put in place to ensure members stay abreast of the changing legal and regulatory issues. Ensuring the right to train AI models on the data you want to use is critical. This is important for companies developing AI tools as well as companies that do fine-tuning or implement retrieval augmented generation with third-party AI tools.

For companies deploying third-party AI tools, it is critical to develop a corporate policy on AI use and adopt an AI vendor diligence process to supplement the standard tech diligence done with acquiring any technology.

AI Use Policy Considerations

Companies using AI tools need an AI use policy to minimize legal liability and loss of rights. The following are just some of the elements to consider for such a policy.

Lawsuits Relating to AI Tools Help to Highlight Key Issues to Consider

The number of lawsuits involving AI is rapidly increasing. The lawsuits include allegations of:

- copyright infringement due to training AI models on copyrighted content and generating output that infringes copyright;
- use of other data to train AI models without the right to do so, including where it exceeds the scope of use in the applicable privacy policy or includes biometric privacy information;
- violation of the right of publicity where the models

are trained on, or the output includes, a person's protected name, image, or likeness;

- failure to maintain copyright management information or otherwise comply with open-source license obligations when using AI code generators;
- biased and discriminatory results or use of AI; and
- defamation where the output of AI is false and harms a person's reputation.

Loss of Valuable Trade Secrets

What some users do not realize is that with many generative AI tools, the inputs are not confidential and so proprietary information may be unknowingly released through their use of AI tools. Even worse, some generative AI tools' terms of use (TOU) expressly grant the tool provider a license to use that input. If the input includes trade secret or sensitive business information, this can lead to losing trade secrets or at least a diminution in the value of the information. Many employees routinely accept the TOU without reading them; thus, they are unaware that they are putting the information at risk.

These issues can extend beyond employee use. For companies that hire outside contractors to create content and other materials, it is important that your contractor agreements address issues with use of generative AI tools on your projects. While many companies have well drafted independent contractor or work-for-hire agreements that address the traditional issues that need to be covered under these arrangements, these agreements need to be updated to address generative AI-related issues.

Inability to Obtain IP Protection for AI-Generated Content

For companies that monetize content, strong IP protection is needed to protect that content. While generative AI excels at cost-effectively creating new content, the problem is that little or no copyright protection is available for generative AI content. The US Copyright Office (Office) has published guidance on registering works that contain AI-generated material.⁶⁴ It states that copyright can protect only material that is the product of human creativity. If a work's traditional elements of authorship (the expressive content) were produced by AI, the work lacks human authorship and the Office will not register it. That a user created the *prompt* to cause the output does not change the result because prompts typically are deemed to be ideas rather than expressions.

Tainting of Proprietary Software Developed with AI Code Generators

Software developers are increasingly using AI code generators. One of the most severe issues, which can adversely affect a company's investment in its software, is called "tainting." Tainting severely devalues software as it requires licensing what you want to be proprietary code under an open-source license. Tainting results from

the conditions in some open-source licenses that require any software that includes or is derived from the open-source software to be licensed under the terms of the open-source license and the source code for that software must be made freely available. For developers who want to license their software under a proprietary license for a fee, tainting negates that possibility. The open-source challenge with AI code generators is that developers often do not know if the code output is newly generated or based on a particular open-source component and if open source, what the applicable license is and whether it can cause tainting or other issues.

Avoiding Bias and Other Issues on the FTC's Watchlist

The FTC has been active in enforcements involving various AI-related issues and issued a report to Congress (Report) warning about various AI issues.⁶⁵ The Report outlines significant concerns that AI tools can be inaccurate, biased, and discriminatory by design and can incentivize relying on increasingly invasive forms of commercial surveillance.

A company's board of directors' obligation to ensure their company avoids bias is not just good corporate citizenship; it is necessary to avoid illegal conduct. Some companies are not aware of the potential for bias in generative AI tools, particularly if they rely on third-party tool providers. In such cases, companies are often unaware of the data on which these tools are trained and whether the data contain or result in biased or discriminatory results.

AI-Related Vendor Diligence

AI-related vendor diligence is critical given the unique issues raised by use of AI tools. Each case may warrant different considerations, but some AI-specific issues to consider include:

1. **Product Documentation and Specifications.** Obtain the product documentation and specifications to understand how the tool uses AI and for what purposes. Confirm what features of the tool leverage AI.
2. **Regulatory Compliance.** Obtain the vendor's policies and procedures for monitoring and ensuring compliance with existing and newly implemented AI-related laws and regulations in all applicable jurisdictions.
3. **Industry Standards.** Determine the vendor's practices for developing, deploying, maintaining, and using the AI tool in accordance with recognized standards and frameworks, including the NIST AI RMF.⁶⁶
4. **Versions.** Are there different versions of the AI tool (e.g., individual/enterprise versions)? If so, what are the different features of each?
5. **Options and Settings.** Determine if the AI tool

includes options or features to mitigate AI legal risks (e.g., filters).

6. **Operation of the Tool.** Make sure you understand the operation of the tool, including:
 - *Inputs/Outputs.* How are inputs and outputs handled? Are they retained for use by the tool for any purpose (e.g., to train the AI model)? Or are they just used to process a request and then deleted? Who owns them?
 - *Disclosure.* Does the AI tool have the ability to automatically mark the output as being AI generated as some jurisdictions are requiring?
 - *Automated Decision-Making.* Does the AI tool perform any automated decision-making on which some regulations limit or impose restrictions?
7. **AI Model.** Determine how the AI model(s) was trained and by whom.
 - Was the training in accordance with responsible AI practices (e.g., the NIST AI RMF or other industry standards)?
 - Where was the model trained? Some countries have more lenient laws relating to training AI in their jurisdiction, but using a tool based on that model may not comply with the laws in the jurisdiction where used.⁶⁷
8. **Training Data.** On what data is the AI model trained? Did the vendor properly acquire the data, and does it have a right to use such data to train the AI model?
9. **License Terms.** What are the license terms and do they vary based on the version? If they vary, make sure you review the correct version of the license. For example, the terms of some free or individual versions of AI tools are often less favorable than those of paid or enterprise versions. The following are some of the issues to consider in reviewing the license:
 - *Infringement Indemnity.* Does the license address infringement indemnity? If so, which party is indemnifying?
 - *Scope.* Review the scope of indemnity and exclusions to assess whether it covers your company for the intended use cases.
 - *Prerequisites to Indemnity.* Check if there are any prerequisites for the indemnity to apply. Some licenses impose obligations on the customer's use of the AI tool for the indemnity to apply.
10. **Testing.** How does the vendor monitor performance of the AI model, including testing output data for accuracy, bias, consistency, and quality? Request information about the process for identifying, modifying, or overriding hallucinations and other flawed or unsatisfactory outputs.

Companies developing AI and using AI vendors need to adopt and implement policies to ensure they apply

responsible AI principles. Consideration of the NIST AI RMF and related documents is helpful, but standing alone it is not enough. The range of issues will vary depending on what the company is developing, but consideration of the issues raised in the FTC CID to OpenAI should also be considered.⁶⁸

Training AI Code Generators on Open-Source Software Raises Other Issues

AI-based code generators are a powerful application of generative AI. These tools leverage AI to assist code developers by using AI models to autocomplete or create code based on human instructions or tests. The models are often trained on software that is licensed under an open-source license. Sometimes, a company can fine-tune using some of its own software. This requires careful consideration of open-source license issues. All companies using open source need an open-source policy and use of AI code generators requires an update to traditional open-source policies.⁶⁹

For example, companies using their own code to fine-tune AI code generators need to consider whether the outputs may include portions of open-source code that adversely affect the company's proprietary software and, even if not, whether the open-source code might impose any compliance obligations. Sometimes, if the code generator outputs any code covered by a restrictive open-source license—e.g., a GNU General Public License (GPL)—then any software including that code may need to be licensed under the GPL. Regarding compliance obligations, many open-source licenses require attribution, maintaining copyright notice, providing notice of modifications, and other obligations. Failure to comply can result in breach and termination of the license. One challenge is knowing when the output code includes open-source code. Some AI code generators have tools such as filters and reference tools to assist with this, but their use is just one element of an effective AI code generator use policy.

For government contractors looking to provide AI solutions to the government, it will be important to understand the policies and guidance outlined above and be able to demonstrate steps taken to ensure transparency, accountability, and nonbiased outcomes. Agencies may require evidence of adequate testing and security as well as continuous monitoring of AI tools throughout the period of use. Where contractors will use AI in performance of a government contract, they should consider informing the customer of such use to avoid any misunderstanding or claim of misrepresentation regarding the method of performance or output.


Conclusion

Executive Order 14110 marks a significant step towards the responsible development and deployment of AI technologies in the United States. By setting forth a framework for governance that emphasizes

trustworthiness and ethical considerations, the Executive Order aims to ensure that AI serves the public good.

Government contractors and other companies will need to align their AI practices with the principles outlined in the Executive Order and associated agency guidance, which may require revamping existing protocols and instituting new policies to ensure compliance. This alignment not only pertains to the technical aspects of AI but also to its ethical considerations, such as bias mitigation and privacy protection.

There is the potential for great opportunity for government contractors as the emphasis on AI in federal budget priorities is likely to spur innovation and investment in the sector. Businesses can expect increased opportunities for partnerships with government agencies, potentially opening new markets and funding sources for AI projects.

For businesses, AI presents both challenges and opportunities that require careful navigation with the help of skilled legal professionals. As we move forward, the legal community will be at the forefront of shaping the future of AI, ensuring that innovation progresses hand in hand with the rule of law. 

Endnotes

1. Exec. Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

2. *Id.*

3. Off. of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights*, WHITE HOUSE (Oct. 4, 2022), <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.

4. *AI Risk Management Framework (RMF) 1.0*, NIST (Jan. 2023), <https://www.nist.gov/itl/ai-risk-management-framework>.

5. Memorandum from Alejandro N. Mayorkas, Sec'y, DHS, to Dr. Dimitri Kusnezov & Eric Hysen, Establishment of a DHS Artificial Intelligence Task Force (Apr. 20, 2023), https://www.dhs.gov/sites/default/files/2023-04/23_0420_sec_signed_ai_task_force_memo_508.pdf.

6. *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, Fed. Trade Comm'n (Apr. 25, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems>.

7. See Press Release, The White House, Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>.

8. Exec. Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

9. *See id.*

10. *See id.*

11. *See id.*

12. Defense Production Act of 1950, Pub. L. No. 81-774, 123 Stat. 2006 (codified at 50 U.S.C. § 4501 et seq.).

13. *See* Exec. Order 14110, 88 Fed. Reg. 75,191.

14. *See id.*

15. Press Release, The White House, Fact Sheet: Biden-Harris Administration Announces Key AI Actions Following President

Biden's Landmark Executive Order (Jan. 29, 2024), <https://www.whitehouse.gov/briefing-room/statements-releases/2024/01/29/fact-sheet-biden-harris-administration-announces-key-ai-actions-following-president-bidens-landmark-executive-order/>.

16. Press Release, The White House, Fact Sheet: Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order (Apr. 29, 2024), <https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/29/biden-harris-administration-announces-key-ai-actions-180-days-following-president-bidens-landmark-executive-order/>.

17. Exec. Order 14110, 88 Fed. Reg. 75,191.

18. *See id.*

19. NIST AI 600-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK: GENERATIVE ARTIFICIAL INTELLIGENCE PROFILE (Apr. 2024), <https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf>.

20. NIST SP 800-218A, SECURE SOFTWARE DEVELOPMENT PRACTICES FOR GENERATIVE AI AND DUAL-USE FOUNDATION MODELS (Apr. 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.ipd.pdf>.

21. NIST AI 100-4, REDUCING RISKS POSED BY SYNTHETIC CONTENT: AN OVERVIEW OF TECHNICAL APPROACHES TO DIGITAL CONTENT TRANSPARENCY (Apr. 2024), <https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent.ipd.pdf>.

22. NIST AI 100-5, A PLAN FOR GLOBAL ENGAGEMENT ON AI STANDARDS (Apr. 2024), <https://airc.nist.gov/docs/NIST.AI.100-5.Global-Plan.ipd.pdf>.

23. For additional information on these documents, see James Gatto, *NIST Updates AI RMF as Mandated by the White House Executive Order on AI*, SHEPPARDMULLIN (Apr. 30, 2024), <https://www.ailawandpolicy.com/2024/04/nist-updates-ai-rmf-as-mandated-by-the-white-house-executive-order-on-ai/>.

24. Colorado Artificial Intelligence Act (CAIA) (S.B. 24-205). For more information on the proposed Colorado legislation, see James G. Gatto, *Colorado Introduces an AI Consumer Protection Bill*, NAT'L L. REV. (Apr. 12, 2024), <https://natlawreview.com/article/colorado-introduces-ai-consumer-protection-bill>.

25. *AI Risk Management Framework (RMF) 1.0*, *supra* note 4.

26. *See* Exec. Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023). The 16 critical infrastructure sectors include Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater Systems. *See also* *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (CISA), <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

27. *See* Exec. Order 14110, 88 Fed. Reg. 75,191.

28. *See id.*

29. *See id.*

30. *See* *Promoting AI Safety and Security*, DEP'T OF HOMELAND SEC. (DHS) (May 13, 2024), <https://www.dhs.gov/ai/promoting-ai-safety-and-security>.

31. DHS, MITIGATING ARTIFICIAL INTELLIGENCE (AI) RISK: SAFETY AND SECURITY GUIDELINES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS (Apr. 2024), https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf.

32. CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE (Nov. 2023), https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf.

33. CISA Proposed Rule, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed.

Reg. 23,644 (Apr. 4, 2024).

34. *See* Press Release, Dep't of Def., DoD Releases AI Adoption Strategy (Nov. 2, 2023), <https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/>.

35. *See* Press Release, DHS, *Fact Sheet: DHS Facilitates the Safe and Responsible Deployment and Use of Artificial Intelligence in Federal Government, Critical Infrastructure, and U.S. Economy* (Apr. 29, 2024), <https://www.dhs.gov/news/2024/04/29/fact-sheet-dhs-facilitates-safe-and-responsible-deployment-and-use-artificial>.

36. Executive Order 14028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26,633 (May 12, 2021).

37. *See* *Open FAR Cases as of June 7, 2024*, DoD, <https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf> (Case No. 2023-002, Supply Chain Software Security).

38. *Secure Software Development Attestation Form*, CISA (rev. Mar. 18, 2024), <https://www.cisa.gov/resources-tools/resources/secure-software-development-attestation-form>.

39. *Artificial Intelligence and Equal Employment Opportunity for Federal Contractors*, Off. of Fed. Cont. Compliance Programs (OFCCP) (Apr. 29, 2024), <https://www.dol.gov/agencies/ofccp/ai-eeo-guide?lang=en>.

40. Memorandum from Jessica Looman, Adm'r, US Dep't of Lab., Artificial Intelligence and Automated Systems in the Workplace Under the Fair Labor Standards Act and Other Federal Labor Standards (Apr. 29, 2024), https://www.dol.gov/sites/dolgov/files/WHD/fab/fab2024_1.pdf.

41. *See* *Responsible Use of Generative Artificial Intelligence for the Federal Workforce*, US Off. of Pers. Mgmt. (OPM), <https://www.opm.gov/data/resources/ai-guidance/>.

42. Exec. Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

43. *See id.*

44. *See id.*

45. NIST AI 100-4, *supra* note 21.

46. Dep't of Comm. Proposed Rule, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, 89 Fed. Reg. 5,698 (Jan. 29, 2024).

47. Memorandum from Shalanda D. Young, Dir., OMB, M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Mar. 28, 2024), <https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf>.

48. Proposed Memorandum from Shalanda D. Young, Dir., OMB, for the Heads of Executive Departments and Agencies, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Nov. 1, 2023).

49. This term refers to "AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of: (1) Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms; (2) Climate or environment, including irreversible or significant environmental damage; (3) Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21 or any successor directive and the infrastructure for voting and protecting the integrity of elections; or, Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government." OMB Memorandum M-24-10, *supra* note 47.

50. This term refers to "AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect on that individual's or entity's: 1. Civil rights, civil liberties,

or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance; 2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or 3. Access to or the ability to apply for critical government resources or services, including health-care, financial services, public housing, social services, transportation, and essential goods and services.” *Id.*

51. *See id.*

52. *Generative AI and Specialized Computing Infrastructure Acquisition Resource Guide*, GEN. SERV. ADMIN. (Apr. 2024), <https://itvmo.gsa.gov/genai/>.

53. FedRAMP, DRAFT PRE-DECISIONAL, EMERGING TECHNOLOGY PRIORITIZATION FRAMEWORK (Jan. 26, 2024), https://www.fedramp.gov/assets/resources/documents/FedRAMP_DRAFT_Emerging_Technology_Prioritization_Framework.pdf.

54. *See AI (and Other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, FED. TRADE COMM’N (FTC) TECH. BLOG (Feb. 13, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive>.

55. For more information on this, see James G. Gatto, *Training AI Models—Just Because It’s Your Data Doesn’t Mean You Can Use It*, NAT’L L. REV. (June 21, 2023), <https://natlawreview.com/article/training-ai-models-just-because-it-s-your-data-doesn-t-mean-you-can-use-it>.

56. *AI (and Other) Companies*, *supra* note 54.

57. *Id.*

58. *Id.*

59. *See* Press Release, Fed. Trade Comm’n, Gateway Learning Settles FTC Privacy Charges: Company Rented Customer Information It Pledged to Keep Private (July 7, 2004), <https://www.ftc.gov/news-events/news/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges>; Press Release, Fed. Trade Comm’n, FTC Says Genetic Testing Company iHealth Failed to Protect Privacy and Security of DNA Data and Unfairly Changed Its Privacy Policy (June 16, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-ihealth-failed-protect-privacy-security-dna-data-unfairly-changed>.

60. For more on this topic, see James Gatto, *FTC Warns About Changing Terms of Service or Privacy Policy to Train AI on Previously Collected Data*, AI LAW & POL’Y (2024), <https://www.ailawandpolicy.com/wp-content/uploads/sites/65/2024/03/FTC-Warns-About-AI-Training-Article-0224.pdf>.

61. Michael Atleson, *Keep Your AI Claims in Check*, FTC BUS. BLOG (Feb. 27, 2023), <https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>.

62. *Id.*

63. *See* FTC, Civ. Investigative Demand (CID) Schedule Issued to OpenAI, FTC File No. 232-3044 (July 13, 2023), available at https://www.washingtonpost.com/documents/67a7081c-c770-4f05-a39e-9d02117e50e8.pdf?itid=lk_inline_manual_4.

64. *See* US Copyright Off., Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16,190 (Mar. 16, 2023), https://copyright.gov/ai/ai_policy_guidance.pdf.

65. FTC, REPORT TO CONGRESS: COMBATTING ONLINE HARMS THROUGH INNOVATION (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combating%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

66. NIST AI 100-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

67. For example, in Japan it is not copyright infringement to train an AI model on third-party copyrighted material. *See Japan*



AMERICAN BAR ASSOCIATION
Public Contract Law Section

Save the Date

Public Contract Law Section Fall Forum & Council Meeting

November 7–8, 2024
CLE Sessions

November 9, 2024
Council Meeting

Hyatt Regency Hotel
Reston, VA

Details and Registration Coming Soon!

Moves to Protect “Copyrights” of AI Creations, JAPAN TIMES (May 10, 2015), <https://www.japantimes.co.jp/news/2016/05/10-national/japan-moves-protect-copyrights-ai-creations/>. However, the EU AI Act states that providers must have a “policy to comply with Union copyright law” (EU AI Act Recitals 104, 107 & art. 53(1)(c), (d)) and “Any provider . . . should comply with this obligation, regardless of the jurisdiction in which the copyright-relevant acts underpinning the training of those general-purpose AI models take place. . . . [N]o provider should be able to gain a competitive advantage in the Union market by applying lower copyright standards than those provided in the Union.” *Id.* Recital 106.

68. For more information on this, see James Gatto, *The Need for Generative AI Development Policies and the FTC’s Investigative Demand to OpenAI*, LAW OF THE LEDGER BLOG (July 15, 2023), <https://www.lawoftheledger.com/wp-content/uploads/sites/15/2023/07/Generative-AI-Development-Policies-Article-0723.pdf>.

69. *See* James G. Gatto, *Open Source Software Policies—Why You Need Them and What They Should Include*, LAW OF THE LEDGER BLOG (June 15, 2019), <https://www.lawoftheledger.com/wp-content/uploads/sites/15/2019/06/Notes-On-Open-Source-Policies-Article-0619.pdf>; James Gatto, *Solving Open Source Problems with AI Code Generators—Legal Issues and Solutions*, LAW OF THE LEDGER BLOG (Aug. 25, 2023), <https://www.lawoftheledger.com/2023/08/articles/artificial-intelligence/solving-open-source-problems-with-ai-code-generators-legal-issues-and-solutions-3/>.