MEALEY'S® LITIGATION REPORT:

Artificial Intelligence

Fine-Tuning Your Policy Statements For The Age Of AI

By
Michael Kearney

Redgrave LLP
Washington, D.C.

and

Judy Branham

Redgrave LLP
Minneapolis, MN

A commentary reprinted from the December 2024 issue of Mealey's Litigation Report: Artificial Intelligence

LexisNexis®

Commentary

Fine-Tuning Your Policy Statements For The Age Of AI

By
Michael Kearney
and
Judy Branham

[Editor's Note: Michael Kearney is Director and Judy Branham is Counsel at Redgrave LLP. Any commentary or opinions do not reflect the opinions of Redgrave LLP or LexisNexis®, Mealey Publications™. Copyright © 2024 by Michael Kearney and Judy Branham. Responses are welcome.]

Barriers to leveraging artificial intelligence systems ("AI systems") have lowered dramatically within the last few years. Powerful computing capabilities that were once the realm of highly trained and funded teams are now widely available. These changes, driven largely by the advancement of generative AI and underlying Large Language Models ("LLMs"), have led to a surge of employees experimenting with AI systems to gain efficiency and improvements at work. Leaders should strive for a balance to harness the benefits of these tools, while protecting their organizations through proper data governance.

This article addresses organizational policy considerations to help strike this balance. While not a survey of the nascent AI governance laws and regulations, the article provides suggestions regarding potential new policy documents to consider, as well as a list of existing policies that should be fine-tuned for the age of AI. The trend of new laws and regulations related to AI systems will undoubtedly continue and organizations should work to get ahead of potential AI governance issues from a policy perspective.

High Level Overview

As the availability of AI systems has increased in the last few years, requirements to properly regulate these systems have also grown. Although at the time of writing, California, Colorado, and Utah are the only states that have enacted major laws regarding the usage of artificial intelligence, debate and passage of related regulation continues throughout the world. The European Union enacted its landmark Artificial Intelligence Act; other countries are beginning to enact their own national laws; the United States is addressing AI at the federal level; and many states have passed smaller, more targeted laws regarding AI.

While looking to address new laws and the deluge of regulation that will undoubtedly follow, an organization should consider the potential need to create an entirely new policy document, as well as the potential need to fine tune existing policies. Most organizations will likely find that appropriate governance of AI systems will require a combination of the two approaches.

New Policy Topics: Governing AI System Risk

The management of risk associated with AI systems is likely an area where organizations will face the need to develop entirely new policy documents. Potential risk surrounding AI is broader than just traditional privacy and security concerns—these systems are non-deterministic, lack complete transparency, and sometimes provide persuasive, yet incorrect (and even offensive) output. These factors are instrumental in driving calls for proper risk management in emerging laws.

Organizations will likely need to develop policies addressing the creation of AI system inventories, the

documentation of risks and related controls for these tools (including training and notification requirements), and identification of individuals tasked with overseeing AI systems. Fortunately, many organizations have built out related governance policies and programs (e.g., data security, privacy, information governance) for digital assets over the last twenty years, and lessons from these endeavors can be applied to AI systems.

Developing Inventories

Before an organization can appropriately assess risk, it must understand and define which technologies fall under the definition of an AI system. Applications and algorithms have existed for decades and organizations have already implemented many policies and controls to govern these tools. The point at which a system raises to the level of "artificial intelligence" is a line that companies will need to address, and this understanding will allow companies to begin to build defensible policies surrounding AI systems.

For most organizations, AI systems are developed by third parties making identification more clear cut. But for internally developed tools, organizations should look to the work already completed by industry and regulatory bodies regarding what constitutes an AI system. The European Union includes in its definition of an AI system a requirement that the technology "operate with varying levels of autonomy" and that it "infers, from the input it receives, how to generate outputs."[1] The United States in its Executive Orders follows the definition of AI provided in 15 U.S.C. 9401(03), which includes usage of inputs for perception of an environment, abstractions of those perceptions into a model, and inferring from the model to create output.[2] Companies should develop a definition of AI systems that takes into account emerging laws, which generally seem to require some type of autonomy, inference, and abstraction to create output.

AI System Assessments and Related Mitigation

Organizations will also likely need to develop new policies that address risks associated with the implementation of AI systems and the appropriate mitigating controls applied to these tools. Emerging laws such as Colorado's Artificial Intelligence Act and the EU AI Act require deployers of AI to conduct an annual assessment for each AI system identified as a "high risk."[3] Accordingly, there is a need to develop policies that will help drive the identification of which AI systems are high risk and the appropriate steps required to adequately mitigate any risk that regulations (and the organization) deem to be too high. Moreover, organizations should assess the need to implement new policies addressing mitigating controls required for both high- and lower-risk AI systems, including any end-user notification and opt-in/opt-out requirements, as well as periodic compliance training for employees. Policies should also identify positions responsible for the maintenance of and compliance with these controls.

Fine Tuning Existing Policies

Many organizations will find that developing a new policy to address AI risk is only one part of the equation to adequately comply with AI governance needs from a policy perspective. Organizations should also review existing related policies to identify potential areas to fine tune for the age of AI systems. Although the structure and breadth of these policies vary among organizations, there are some general areas for which most organizations already maintain policies.

Confidentiality

With the release of ChatGPT in late 2022, many organizations immediately raised concerns regarding the protection of sensitive information when using AI tools. One of the main issues relates to generative AI tools that use data provided by the end-user to help train an underlying LLM. Once used in the training, it may be impossible to remove the underlying content from the LLM and that underlying content could be used to help inform answers provided to other users of the tool. In short, sensitive information entered into a generative AI tool could potentially be exposed to other users. This concern drove initial prohibitions of AI tools at many companies.[4]

But as AI tools become more pervasive and organizations begin to weigh operational benefits, complete prohibitions may not be practicable. Organizations open to allowing users to leverage AI systems should update confidentiality policies to include guidance regarding the appropriate usage of these tools. Policy statements should clearly outline approved tools and the types of data that an employee may enter into these tools. For example, a policy might only allow

employees to enter sensitive information into a specific AI system, for which the organization has a contract and has gone through the required organizational approval process. Policies should further remind employees of their confidentiality obligations and include additional training when deemed necessary.

Security and Privacy Policies

The adoption of AI systems should fit within existing security and privacy frameworks already developed by organizations. The implementation and usage of these tools should follow already established information security and privacy risk assessments and practices. The "monitor and update" phases of these programs should provide an adequate mechanism to update security and privacy policies to address additional concerns introduced by the influx of AI systems. For example, organizations will likely need to revisit security policies addressing operations, configuration, development, and incident response to ensure the proper handling of new threats or vulnerabilities. Moreover, organizations should revisit privacy policies to ensure continued appropriate handling and access guidance and controls, as well as the need for any additional notification language required for customers and employees.

Conclusion

Beyond the highlighted AI risk, confidentiality, security, and privacy policies, an organization should consider review of all data-related policies to determine any need for additional language to address AI systems. The usage of these tools in the workplace is here to stay in one form or another. Organizations that proactively address AI from a policy standpoint will find it easier to find a balance between productivity gains from usage of these tools and the need for appropriate information governance.

Endnotes

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (EU AI Act), Article 3(1) (defining "AI system").

2. *See, e.g., Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, The White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

3. S.B. 24-205, Gen. Assem., at 6-1-1703 (I). EU AI Act, 58.

4. For example, a major electronics company in 2023 forbade its employees from using chatbots in response to sensitive internal source code that was entered into ChatGPT. Siladitya Ray, *Samsung Bans ChatGPT Among Employees After Sensitive Code Leak*, Forbes (May 2, 2023), https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/. ■

MEALEY'S LITIGATION REPORT: ARTIFICIAL INTELLIGENCE
edited by Bryan Redding
The Report is produced monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: lexisnexis.com/mealeys
ISSN 2994-1105