protiviti®
Global Business Consulting

White House Issues Executive Order to "Seize the Promise and Manage the Risks" of AI

November 1, 2023

In his first executive order (EO) on artificial intelligence (AI), President Biden is directing various federal agencies to identify the risks of the technology as well as harness the benefits. This is something to watch because the details will be important – regulatory and legislative changes are coming.

Key Directives in the Executive Order

Among the key directives government agencies need to address, per the EO, are the following:

- Directing the development of new standards and rules across federal agencies
- Initiating action to address the most concerning implications of the broad adoption of AI in public and private sectors
- Catalysing research and assistance across impacted ecosystems
- Calling on Congress to pass a Federal Privacy Bill
- Aligning with other global actions (G7, European Union Artificial Intelligence Act, etc.)

Numerous Questions Remain

Despite efforts to be as comprehensive as possible, the EO raises several questions that will need to be addressed before businesses can fully determine the impact that forthcoming EO implementation may have.

- How is "safety" defined and by whom?
- How will AI developers and users demonstrate that models are free of discrimination and bias?

- How will small- to medium-sized businesses navigate the new rules and regulations (domestic and international) given the "moat" that may already exist around big tech players?
- How do forthcoming standards apply to AI solutions already in use versus newly developed ones?
- How will this impact the balance between regulation and free speech?

There are other concerns that business leaders need to be aware of; for example, how the open-source community and those that leverage open-source AI tools and models will be impacted. A significant open-source presence already exists with no single corporate entity responsible for development. Currently, more than 225 transformer models (the architecture behind the wildly popular ChatGPT) are available on the popular open-source AI community, HuggingFace, with more to come. These models are also being made widely available through hyperscalers such as AWS and GCP.

Key Takeaways and Concerns

- **Standardisation is key**: The initiative's ultimate success will depend on the ability of a multitude of agencies to put in place essential definitions, guardrails and regulations necessary to provide sufficient guidance to enable the power of AI while navigating both known and unknown risks. New AI safety and security standards will be developed for powerful AI systems, intended to apply to certain models that pose a serious risk to national security, national economic security, or national health and safety.
- **Definition of safe**: The EO directs NIST to develop standards, tools and tests for safe systems. However, there remains a lack of specific guidance on what constitutes a safe system, and the directive fails to distinguish between the risks presented by AI software and the combination of AI software and hardware.
- **Safety testing**: The developers of these powerful AI systems may be required to share critical information with the federal government; specifically, "developers of foundation models must share the results of all red-team safety tests." Traditionally, red-team safety tests focus on manipulating a model (through simulated adversarial attacks), not necessarily on whether the model is inherently biased, safe or responsible. As noted above, those determinations depend on standardised definitions and evaluation mechanisms.

- **AI-generated content labelling**: To address fraudulent and deceptive uses of AI, the EO directs the Department of Commerce to develop standards and best practices for detecting and authenticating official content, including watermarks to distinctly label AI-generated content. This proactive measure could be a powerful tool in distinguishing between content created by humans and that produced by AI; however, technology to detect AI-generated content is still a work in progress. As of July 20, 2023, OpenAI revoked its technology intended to detect AI-written text and stated that its "AI classifier is no longer available due to its low rate of accuracy."

- **Federal privacy law**: The EO calls on Congress to pass bipartisan privacy legislation to protect all citizens and asserts that federal support and the development of privacy-preserving technology should be prioritised. It also establishes a new "Research Coordination Network" to advance rapid breakthroughs in privacy. As AI technology continues to evolve, the EO turns the privacy lens on the government by directing an evaluation of how agencies collect and use commercially available information and personally identifiable data. Privacy serves as a double-edged sword for AI – large amounts of data (which may include sensitive information) may be required to train models, which may represent risk to individuals' personal data.

- **Mitigating bias**: The EO directs government agencies to take steps to address algorithmic bias and discrimination related to AI systems, calling for the development of guidance and best practices for mitigating algorithmic discrimination, ensuring AI systems comply with civil rights laws, conducting evaluations to detect unjust impacts on protected groups, and granting human consideration for adverse decisions made by AI systems. It further directs the Department of Justice to coordinate civil rights enforcement regarding AI discrimination. Also of note, the EO encourages the Director of the Federal Housing Finance Agency and the Director of the Consumer Financial Protection Bureau to consider using their authorities to use appropriate methodologies, including AI tools, to ensure compliance with federal law. This includes evaluating their underwriting models for bias or disparities affecting protected groups and evaluating automated collateral valuation and appraisal processes.

These broad mandates underscore the federal government's determination to protect core national interests. An intriguing aspect of these proposed standards is their reliance on

existing agency enforcement. Unlike some other jurisdictions that have introduced specific AI regulatory bodies, the standards do not create new enforcement agencies or mechanisms.

What Businesses Can Do to Prepare for Changes in the AI Regulatory Landscape

While much work remains to be done before the EO has an appreciable impact on how businesses use AI, some preparatory steps will still prove beneficial for those developing and deploying AI.

1. Establish an AI code of ethics aligning with your corporate ethics and mission.
2. Develop an inventory of AI/ML systems and a repository of algorithms, documenting each model's purpose, data sources, key parameters and business context.
3. Formalise an AI governance structure, including roles and responsibilities, and plans for red teaming and auditing.
4. Evaluate AI products/services and uses against a standard framework such as the NIST AI Risk Management Framework.

Closing Thoughts

While the success of the EO is contingent on the development and execution of plans and policies by government agencies, the EO indicates there is growing public awareness of the potential privacy, ethical and security challenges presented by AI and the need to address those. Taking the suggested steps above will help businesses futureproof themselves for forthcoming regulations, and ultimately will help businesses better leverage the capabilities of AI.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®