LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Know About The White House's Sweeping AI Directive

By **Allison Grande**

Law360 (October 30, 2023, 11:21 PM EDT) -- President Joe Biden signed a comprehensive executive order Monday that sets out a road map for protecting consumers and workers from privacy, discrimination and other potential harms presented by the widespread deployment of artificial intelligence, but experts say its effectiveness will likely hinge on how the directive is implemented and whether it's backed up by congressional action.

The long-awaited executive order establishes new standards for AI safety, security and innovation across a range of industries, including technology, banking, education, health care, housing and the workplace. The 100-plus-page document requires federal agencies and developers of certain AI technologies to take steps to improve privacy and transparency and protect civil rights, while boosting research and diplomacy efforts aimed at promoting competition and advancing U.S. leadership in the rapidly evolving field.

While the executive order won praise from a slew of lawmakers, consumer advocates and policy experts, some expressed concerns that it would ultimately end up lacking its intended bite.

"While this is a major action on AI, and includes some critical components on addressing discrimination and bias, what comes next is really the story," Caitlin Seeley George, campaigns and managing director at digital rights advocacy group Fight for the Future, told Law360.

"In the best-case scenario, agencies take all the potential actions that could stem from the executive order and use all their resources to implement positive change for the benefit of everyday people," she added. "But there's also the possibility that agencies do the bare minimum, a choice that would render this executive order toothless."

Observers also pointed to issues with the natural limitations of executive orders. They can't go as far as congressional legislation, which would be able to establish new rules in this area and address issues outside those that impact the government.

"As much as the White House can do on its own, those measures are no substitute for agency regulation and legislative action," said Robert Weissman, the president of Public Citizen, a progressive consumer rights advocacy group and think tank. "Preventing the foreseeable and unforeseeable threats from AI requires agencies and Congress take the baton from the White House and act now to shape the future of AI — rather than letting a handful of corporations determine our future, at potentially great peril."

Several lawmakers Monday pledged action on AI, including Senate Majority Leader Chuck Schumer, D-N.Y.

"This is a massive step forward, but of course more is needed," Schumer said in a statement. "All executive orders are limited in what they can do, so it is now on Congress to augment, expand and cement this massive start with legislation."

The majority leader said the Senate would continue to work "in bipartisan fashion, in conjunction with the president and his administration, to build upon this momentum," and urged his colleagues to act "with urgency and humility" in this area.

"Urgency because we can't wait while other countries are gaining on us, and humility because the task of ensuring sustained investment to advance AI innovation and setting commonsense guardrails is a powerful and challenging one," Schumer said. "We cannot afford to wait."

"Both Sweeping and Specific"

In reacting to the executive order, the first move made by U.S. Sen. Mark Warner, a Virginia Democrat who chairs the Senate Select Committee on Intelligence and co-chairs the chamber's cybersecurity caucus, was to note how he was "impressed by the breadth" of the order.

Aside from tackling issues such as the privacy risks posed by companies amassing vast quantities of data to train AI models and discrimination and bias issues in the housing, employment and health care fields, the executive order also notably devotes sections to topics that promote the use of this technology, increasing the AI workforce, federal procurement and global engagement on these issues, Warner noted.

Weissman of Public Citizen described the executive order as being "both sweeping and specific, covering the vast implications of AI for the government and society and directing agencies to pursue a long list of specific policies and principles."

To promote safety and security, the executive order requires the U.S. Department of Commerce's National Institute of Standards and Technology to establish rigorous standards for extensive red team testing, which will need to be carried out and reported by companies developing "any foundation model that poses a serious risk to national security, national economic security or national public health and safety." Red team testing is a security testing method in which the participants pretend to hack an organization's systems in order to test the strength of their cyberdefenses.

The U.S. Department of Homeland Security will be charged with establishing an AI Safety and Security Board and applying those standards to critical infrastructure sectors to ensure that AI systems are safe, secure and trustworthy before companies make them public.

While the application of these standards is limited to critical infrastructure, Dan Felz, a partner at Alston & Bird LLP, noted that Cybersecurity and Infrastructure Security Agency considers the term to be quite broad, covering companies in sectors such as financial services, healthcare, telecommunications and IT.

"That could mean that mandatory AI testing could become more widespread than anticipated," Felz said. "As we often discuss with companies, this is simply one more reason to get started inventorying

the AI in use across the organization, as federal agencies are also required to do under prior executive orders."

Additionally, Commerce will be tasked with developing guidance for content authentication and watermarking to clearly label AI-generated content, and the U.S. Patent and Trademark Office has been directed to clarify key issues at the intersection of intellectual property and artificial intelligence.

Within 120 days, the USPTO director will need to publish guidance to patent examiners and applicants addressing "inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed."

The director will also have 270 days to issue additional guidance on "other considerations at the consideration of AI and IP," which could include updated guidance on patent eligibility. Additionally, the USPTO will need to issue recommendations on potential executive actions that the White House could take related to copyright and AI issues. That report must be done either within 270 days or within 180 days of the U.S. Copyright Office publishing its forthcoming study on the issue, whichever comes first.

The executive order also directs several federal agencies to craft policies and best practices to address a range of bias and discrimination concerns raised by AI technologies.

These actions include requiring the U.S. Department of Labor to develop principles to mitigate potential harms from AI-based tracking of workers' activities and productivity, and directing the U.S. Department of Housing and Urban Development and the Consumer Financial Protection Bureau to come up with guidance on how the use of algorithmic tenant screening and algorithmic targeting of advertising for housing and credit can lead to discriminatory outcomes that violate existing laws.

Additionally, the U.S. Department of Health and Human Services and the U.S. Department of Agriculture will be required to exercise their authority to ensure that use of AI doesn't undermine the equitable administration of government programs and benefits, according to the executive order.

"This executive order represents a remarkable, whole-of-government effort to support the responsible development and governance of AI," Alexandra Reeve Givens, president and CEO of the Center for Democracy and Technology, told Law360. "It's notable to see the administration focus on both the emergent risks of sophisticated foundation models and the many ways in which AI systems are already impacting people's rights."

Dina Blikshteyn, a partner at Haynes and Boone LLP, noted that the executive order builds on several previous government initiatives in this space, including its issuance last year of an AI Bill of Rights, which lays out a road map for the safe and responsible use of the technology, and its announcement in July that it had secured commitments from seven leading AI companies — Amazon, Anthropic, Google, Inflection, Meta Platforms, Microsoft and OpenAI — to support the safe and responsible deployment of AI, including boosting their investment in cybersecurity and being more transparent about how this technology is being used.

"Nearly every industry is trying to implement generative AI in some way, shape or form, and that also comes with issues," Blikshteyn said. "The White House has clearly shown it's looking at this issue, and this executive order provides insight into where it's going and gives companies a document it can almost use as a guide about what it can and should be doing right now."

Blikshteyn specifically pointed to the steps the executive order takes to address privacy issues, which are among the most pressing, given the vast quantities of data that are needed to train effective AI models. The executive order directs the government to prioritize federal support and research for accelerating the development and use of privacy-preserving techniques that allow models to be trained while still preserving individuals' data privacy.

Jodi Daniel, who served as the head of health information technology policy for HHS for a decade, highlighted the order's language on privacy-preserving technologies and pointed out the large quantity of data required in developing AI technology.

"Developing technology that will enable the use of that data while mitigating risk to the privacy of the individual whose data might be used in that development — I think it's really important," said Daniel, who is now a partner at Crowell & Moring LLP.

Implementation Will Be Key

Given the breadth of the executive order, the Biden administration appears to have chosen to tackle AI by "adopting an everything-and-the-kitchen-sink approach to AI policy that is, at once, extremely ambitious and potentially overzealous," noted Adam Thierer, a senior fellow for the R Street Institute's technology and innovation team.

"The implementation details on all the matters here are mostly left to the various federal agencies to work out, and it remains unclear how far they can stretch their statutory authority to enforce many of these stipulations," Thierer said.

With the executive order heavily reliant on federal agencies to set certain benchmarks and standards across various sectors and industries, the directive's success will undoubtedly "rely on its effective implementation," according to the Center for Democracy and Technology's Givens, who urged the Biden administration "to move quickly to meet relevant deadlines, and to ensure that any guidance or mandates issued under the EO are sufficiently specific and actionable to drive meaningful change."

The National Institute of Standards and Technology, which is charged with leading technical work to develop industry standards for the safe and responsible development of AI models, creating test environments to evaluate these systems and developing standards on privacy and authentication of AI-generated content, on Monday pledged to work with private and public stakeholders to carry out its responsibilities under the executive order.

"We are committed to developing meaningful evaluation guidelines, testing environments and information resources to help organizations develop, deploy and use AI technologies that are safe and secure, and that enhance AI trustworthiness," Under Secretary of Commerce for Standards and Technology and NIST Director Laurie Locascio said in a statement.

Advocacy groups like the Center for Democracy and Technology and the Electronic Privacy Information Center, which also applauded the White House for its "landmark" executive order, expressed similar sentiments.

"EPIC looks forward to working with federal agencies to carry out the Executive Order and ensure that artificial intelligence systems reflect our fundamental values and serve the public interest," the group's

Executive Director Alan Butler said.

The Center for Data Innovation also expressed optimism about the executive order's potential, with senior policy analyst Hodan Omaar noting that the directive "sets a clear course" for the U.S. and "provides industry with long-awaited guidance for AI oversight, including advising tech companies to adhere to the NIST AI risk management framework, watermark AI-generated content, consider the data used in model training and incorporate red teaming into testing."

"However, while the general direction for AI oversight is clear, the specifics of implementation remain uncertain, which means both companies and regulators will need to navigate uncharted waters," Omaar said, noting that the executive order calls for new standards on topics that "are all active areas of research where there are no simple solutions," such as detecting AI-generated content and using AI for biological engineering.

"Policymakers often forget that the reason industry hasn't already adopted certain solutions is because those solutions don't yet exist," Omaar said.

Another area that could prove tricky is developing standards for tackling discrimination and bias in housing, employment, health care, banking and other vital areas, noted Dion M. Bregman, a partner at Morgan Lewis & Bockius LLP.

"Ensuring fairness and equity in AI systems is a complex and evolving challenge," he said, adding that "the effectiveness of these measures in practice remains to be seen."

Only a First Step

While praising the executive order, Warner, the Democratic senator from Virginia, noted that there's still work to be done.

He argued that many of the provisions, particularly in areas like health care and competition policy, "just scratch the surface," while "other areas overlap pending bipartisan legislation, such as the provision related to national security use of AI, which duplicates some of the work in the past two Intel Authorization Acts related to AI governance."

"While this is a good step forward, we need additional legislative measures, and I will continue to work diligently to ensure that we prioritize security, combat bias and harmful misuse, and responsibly roll out technologies," Warner said in a statement.

In issuing the executive order Monday, the Biden administration acknowledged that "more action will be required" and pledged "to continue to work with Congress to pursue bipartisan legislation to help America lead the way in responsible innovation." These proposals include ones that specifically tackle the privacy and discrimination risks posed by AI, as well as comprehensive proposals that would more broadly regulate how companies collect, use and disclose a broad range of personal information.

"Recognizing that comprehensive federal privacy legislation could help spur continued development of artificial intelligence, the administration smartly calls for Congress to pass such legislation acknowledging that artificial intelligence development and deployment increases incentives to collect, use and share more data as AI models require data for training," Gerry Stegmaier, a partner at Reed Smith LLP, told Law360.

EPIC's Butler likewise said a robust privacy law was necessary to counter the growing "incentives" that companies have "for capturing personal data on a massive scale," which are being fueled by AI.

"Artificial intelligence and privacy are inextricably linked," Butler said. "Without a strong privacy law, there will be no meaningful limits on how companies collect and use our data for artificial intelligence systems."

--Additional reporting by Gianna Ferrarin. Editing by Alanna Weissman and Michael Watanabe.
