Joe Biden moves to compel tech groups to share AI safety test results

By Stefania Palma & John Hammond – October 2023

Companies whose artificial intelligence models could threaten US national security will have to share how they are ensuring the safety of their tools under a sweeping order by Joe Biden intended to curb the risks posed by the technology.

The order is the broadest step taken by the administration so far in tackling AI threats, from national security to competition and consumer privacy. The measure seeks to mobilize agencies across Washington, including the departments of commerce, energy and homeland security. “To realize the promise of AI and avoid the risk, we need to govern this technology, there’s no way around it,” Biden told an event at the White House on Monday.

“President Biden is rolling out the strongest set of actions any government in the world has ever taken on AI safety, security and trust,” said Bruce Reed, White House deputy chief of staff. “It’s the next step in an aggressive strategy to do everything on all fronts to harness the benefits of AI and mitigate the risks.”

The order comes as countries across the world grapple with how to regulate AI companies and models that are not naturally captured by individual watchdogs. Gary Gensler, chair of the US Securities and Exchange Commission, told the Financial Times recently that a financial crisis was “nearly unavoidable” within a decade if regulators failed to manage AI risks.

The measures come two days before vice-president Kamala Harris, the Biden administration’s AI tsar, is set to give a speech in London about US policy, before attending the UK’s Bletchley Park summit, where world leaders and tech company executives will discuss potential ground rules for the development of “frontier AI”.

“We intend that the actions we are taking domestically will serve as a model for international action,” Harris told the White House event. She pledged to work with other countries “to apply existing international rules and norms with a purpose to promote global order and stability, and where necessary to build support for additional rules and norms which meet this moment”.

The EU has moved rapidly, drafting tough measures over the use of the technology in a groundbreaking law that is set to be fully approved by the end of the year. But the US is still assessing which aspects of it require new regulation and what is subject to existing statutes.

Asked if the EU law had influenced Biden’s order, a senior administration official said: “I don’t think we’re in a race. I don’t think we’re playing catch-up.” The US had liaised with the EU and a “wide range” of the bloc’s member states about AI regulation, the official added.

Leading industry figures including OpenAI co-founder Sam Altman have toured the globe this year to discuss the potential impact of the tools they are developing. Altman and others have struck a conciliatory tone with regulators but resisted calls to stall or slow the development of increasingly powerful AI.

In May, Altman said his company could “cease operating” in Europe if Brussels’ efforts to regulate the technology were overly stringent. He later walked back the comments.

Biden’s order escalates US AI policy after 15 companies — including Amazon, Google, Meta, Microsoft and OpenAI — made voluntary commitments earlier this year to manage the technology’s risks. The White House will use the Defense Production Act, a cold war law used at the peak of the Covid-19 pandemic, to compel businesses developing AI models posing serious risks to national security, economic security, or public health to notify the government when training these systems and to share their safety test results.

To date, companies vying for AI dominance have typically preferred to keep the designs of their models private. “If organizations don’t adhere to that law, we could bring Department of Justice actions in appropriate manner to enforce that,” said the senior official. But he stressed that these requirements would “primarily” capture the next generation of the world’s most powerful AI tools and would not “catch any system currently on the market”.

Under the order, the commerce department must craft guidance on adding watermarks to AI-generated content in a bid to tackle “fraud and deception”, including deepfakes.

The measures also seek to promote competition in the AI sector and encourage the Federal Trade Commission “to exercise its authorities” at a time when US antitrust regulators have warned against potential monopolies arising from the technology’s structural dependence on scale.

The order addresses privacy risks, urging Congress to pass data privacy legislation while seeking an assessment of how agencies collect and use “commercially available information”. It also calls for measures to curb harms caused by AI on workers and medical patients as well as to address “algorithmic discrimination” in housing, healthcare and justice.

The senior official said that while executive orders “have the force of law”, Biden has said “that we were going to need bipartisan legislation to do more in artificial intelligence”. Many of the president’s priorities “require legislative action to fully execute.”

Source: https://www.ft.com/content/3c6fb9ef-4185-4157-943c-5142ab4dc2f7

I- Comprehension questions

1- Why did Joe Biden issue the sweeping order regarding artificial intelligence?
a) To promote international competition
b) To limit the involvement of agencies in AI-related matters
c) To encourage the development of powerful AI tools without restrictions
d) To address concerns related to national security, competition, and consumer privacy

2- According to Bruce Reed, what does President Biden's order represent in terms of government actions on AI?
a) The weakest set of actions
b) The most aggressive strategy to harness AI benefits and mitigate risks
c) A moderate approach to AI safety and security
d) No significant impact on AI policy

3- Which agencies across Washington are mentioned as part of the mobilization efforts in response to the AI threats?
a) The departments of commerce, energy, and homeland security
b) The departments of education, defense, and justice
c) The departments of health, environment, and transportation
d) The departments of state, agriculture, and labor

4- Why is the EU mentioned in the context of AI regulation?
a) The EU has already fully approved groundbreaking laws on AI.
b) The EU is influencing Biden's order, leading to a competitive race.
c) The US and the EU are collaborating on international AI norms.
d) The EU has resisted AI regulation, unlike the US.

5- How does the Biden administration plan to use the Defense Production Act in relation to AI?
a) To encourage voluntary commitments from AI companies
b) To impose strict regulations on AI development
c) To compel businesses to share information on AI models posing risks
d) To restrict the export of AI technologies

II – Right or Wrong questionnaire. Justify by quoting from the text

6- The EU's groundbreaking law on AI is fully approved by the time of the article.

7- OpenAI co-founder Sam Altman has expressed willingness to slow down the development of powerful AI tools.

8- The Defense Production Act will primarily target existing AI systems already on the market.

9- The commerce department is tasked with addressing privacy risks by urging companies to add watermarks to AI-generated content.

10- According to the senior official, executive orders alone can fully address President Biden's priorities in artificial intelligence.

III – Vocabulary exercise

11- President Biden's order on artificial intelligence seeks to _____ agencies across Washington to address the risks posed by the technology.

Options: a) mobilize, b) scrutinize, c) marginalize, d) epitomize

12- The EU has drafted _____ measures over the use of AI in a groundbreaking law set to be fully approved by the end of the year.

Options: a) obsolete, b) lenient, c) sporadic, d) stringent

13- OpenAI co-founder Sam Altman has toured the globe to discuss the potential _____ of the tools they are developing.

Options: a) drawbacks, b) ramifications, c) precedents, d) anomalies

14- The Defense Production Act will _____ businesses developing AI models posing serious risks to national security.

Options: a) relinquish, b) mitigate, c) compel, d) exacerbate

15- The order emphasizes the importance of data privacy legislation to _____ individuals' privacy rights.

Options: a) safeguard, b) jeopardize, c) infringe, d) neglect

16- The Federal Trade Commission is encouraged to exercise its authorities to promote _____ in the AI sector.

Options: a) stagnation, b) innovation, c) proliferation, d) retrogression

17- AI companies must bear _____ for the safety and security of their technologies.

Options: a) responsibility, b) recklessness, c) apathy, d) nonchalance

18- The order addresses privacy risks and urges Congress to pass data privacy legislation while seeking an _____ of how agencies collect and use information.

Options: a) abatement, b) enhancement, c) assessment, d) dispersion

10- The order calls for measures to curb harms caused by AI and address "algorithmic _____" in housing, healthcare, and justice.

Options: a) parity, b) equity, c) discrimination, d) conformity

20- President Biden's order escalates US AI policy after 15 companies made _____ commitments earlier this year to manage the technology's risks.

Options: a) obligatory, b) voluntary, c) compulsory, d) mandatory