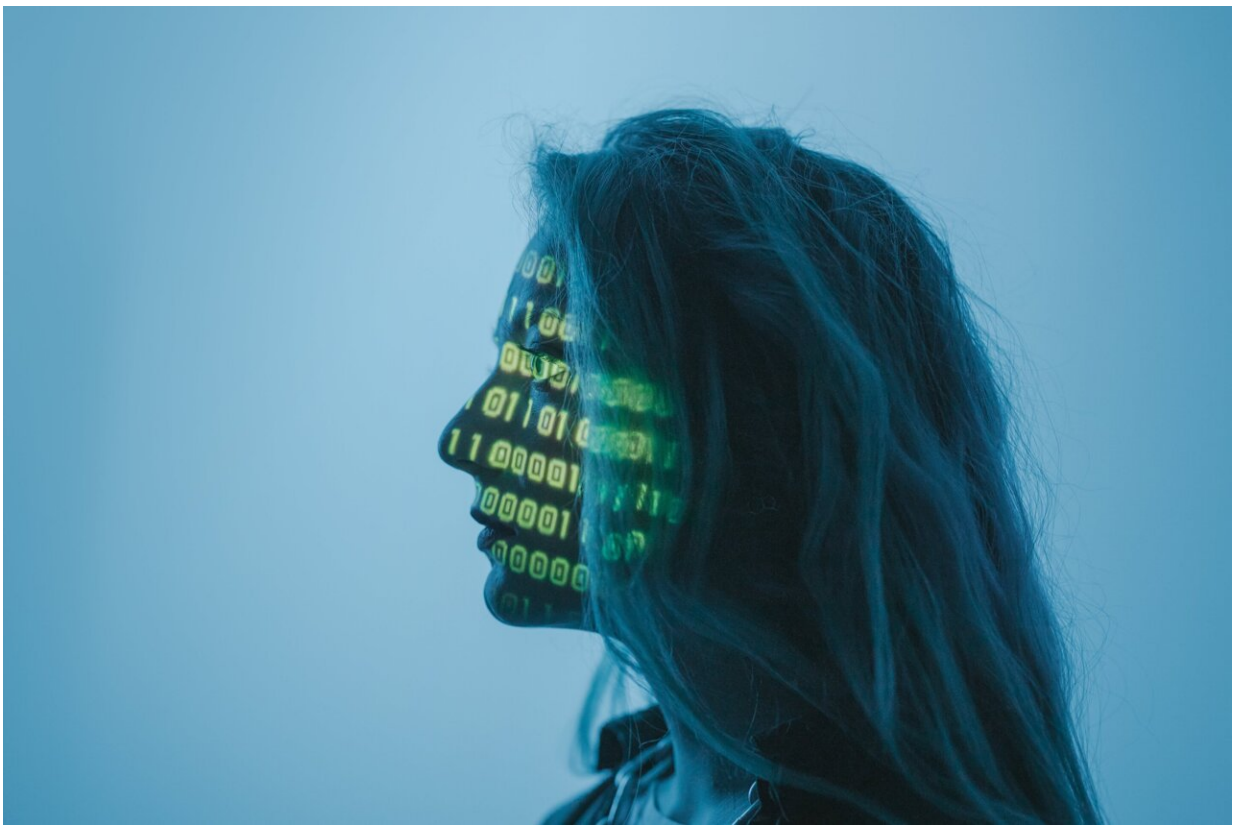
The US just issued the world's strongest action yet on regulating AI. Here's what to expect

October 31 2023, by Toby Walsh



Credit: cottonbro studio from Pexels

On Monday US President Joe Biden released a wide ranging and ambitious executive order on artificial intelligence (AI)—catapulting the

US to the front of conversations about regulating AI.

In doing so, the US is leap frogging over other states in the race to rule over AI. Europe previously led the way with its AI Act, which was passed by the European Parliament in June 2023, but which won't take full effect until 2025.

The presidential executive order is a grab bag of initiatives for regulating AI—some of which are good, and others which seem rather half-baked. It aims to address harms ranging from the immediate, such as AI-generated deepfakes, through to intermediate harms such as job losses, to longer-term harms such as the much-disputed existential threat AI may pose to humans.

Biden's ambitious plan

The US Congress has been slow to pass significant regulation of big tech companies. This presidential executive order is likely both an attempt to sidestep an often deadlocked Congress, as well as to kick-start action. For example, the order calls upon Congress to pass bipartisan data privacy legislation.

Bipartisan support in the current climate? Good luck with that, Mr. President.

The executive order will reportedly be implemented over the next three months to one year. It covers eight areas:

1. safety and security standards for AI
2. privacy protections
3. equity and civil rights
4. consumer rights
5. jobs

6. innovation and competition
7. international leadership
8. AI governance.

On one hand, the order covers many concerns raised by academics and the public. For example, one of its directives is to issue official guidance on how AI-generated content may be watermarked to reduce the risk from deepfakes.

It also requires companies developing AI models to prove they are safe before they can be rolled out for wider use. President Biden said: "That means companies must tell the government about the large scale AI systems they're developing and share rigorous independent test results to prove they pose no national security or safety risk to the American people."

AI's potentially disastrous use in warfare

At the same time, the order fails to address a number of pressing issues. For instance, it doesn't directly address how to deal with killer AI robots, a vexing topic that was under discussion over the past two weeks at the General Assembly of the United Nations.

This concern shouldn't be ignored. The Pentagon is developing swarms of low-cost autonomous drones as part of its recently announced Replicator program. Similarly, Ukraine has developed homegrown AI-powered attack drones that can identify and attack Russian forces without human intervention.

Could we end up in a world where machines decide who lives or dies? The executive order merely asks for the military to use AI ethically, but doesn't stipulate what that means.

And what about protecting elections from AI-powered weapons of mass persuasion? A number of outlets have reported on how the recent election in Slovakia may have been influenced by deepfakes. Many experts, myself included, are also concerned about the misuse of AI in the upcoming US presidential election.

Unless strict controls are implemented, we risk living in an age where nothing you see or hear online can be trusted. If this sounds like an exaggeration, consider that the US Republican Party has already released a campaign advert which appears entirely generated by AI.

Missed opportunities

Many of the initiatives in the executive order could and should be replicated elsewhere, including Australia. We too should, as the order requires, provide guidance to landlords, government programs and government contractors on how to ensure AI algorithms aren't being used to discriminate against individuals.

We should also, as the order requires, address algorithmic discrimination in the criminal justice system where AI is increasingly being used in high stakes settings, including for sentencing, parole and probation, pre-trial release and detention, risk assessments, surveillance and predictive policing, to name a few.

AI has controversially been used for such applications in Australia, too, such as in the Suspect Targeting Management Plan used to monitor youths in New South Wales.

Perhaps the most controversial aspect of the executive order is that which addresses the potential harms of the most powerful so-called "frontier" AI models. Some experts believe these models—which are being developed by companies such as Open AI, Google and

Anthropic—pose an existential threat to humanity.

Others, including myself, believe such concerns are overblown and might distract from more immediate harms, such as misinformation and inequity, that are already hurting society.

Biden's order invokes extraordinary war powers (specifically the 1950 Defense Production Act introduced during the Korean war) to require companies to notify the federal government when training such frontier models. It also requires they share the results of "red-team" safety tests, wherein internal hackers use attacks to probe a software for bugs and vulnerabilities.

I would say it's going to be difficult, and perhaps impossible, to police the development of frontier models. The above directives won't stop companies developing such models overseas, where the US government has limited power. The open source community can also develop them in a distributed fashion—one which makes the tech world "borderless."

The impact of the executive order will likely have the greatest impact on the government itself, and how it goes about using AI, rather than businesses.

Nevertheless, it's a welcome piece of action. The UK Prime Minister Rishi Sunak's AI Safety Summit, taking place over the next two days, now looks to be somewhat of a diplomatic talk fest in comparison.

It does make one envious of the presidential power to get things done.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: The US just issued the world's strongest action yet on regulating AI. Here's what to expect (2023, October 31) retrieved 15 April 2024 from https://techxplore.com/news/2023-10-issued-world-strongest-action-ai.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.