Q&A: Biden's executive order on AI brings awareness to emerging technology but lacks enforcement mechanism

October 31 2023, by Cesareo Contreras

Credit: Unsplash/CC0 Public Domain

President Joe Biden has issued a sweeping executive order aimed at steering the development of artificial intelligence technologies. It's the first order of its kind to come out of the federal government directly related to regulating the emerging technology.

The new directive provides standards and guidance on a number of focus areas, including safety and security, privacy, equity and civil rights, consumer and worker protections, research, competition and innovation, work abroad and governmental use of AI.

As part of the new order, and in accordance with the Defense Production Act, AI companies will be required to share the safety test results of new AI models with the federal government before they are released.

Additionally, the National Institute of Standards and Technology will create new "standards, tools, and tests" for companies to use while stress-testing their AI systems for vulnerabilities and other security issues as part of a practice called "red teaming."

Those standards will be enforced by the Department of Homeland Security, which is in the process of establishing an AI Safety and Security Board as part of the order. The Department of Homeland Security will also collaborate with the Department of Energy to "address AI systems' threats to critical infrastructure, as well as radiological, nuclear and cybersecurity risks," according to the order.

Additionally, the order establishes the creation of a new safety program to be run by the U.S. Department of Health and Human Services designed "to receive reports of—and act to remedy—harms or unsafe health care practices involving AI."

These are just a few of the highlights of the new directive, which the Biden administration says builds on conversations it's had with 15 leading AI companies that have voluntarily pledged to "drive safe, secure, and trustworthy development of AI." Google, Microsoft and Open AI are among the companies that have made the pledge.

Usama Fayyad, executive director of Northeastern's Institute for

Experiential AI, spoke with Northeastern Global News about the pros and cons of the new order. This interview has been edited for brevity and clarity:

This order covers a lot of different aspects of AI development and deployment. What specific actions in the order stand out to you?

The standout actions are the ones that basically say, "Let's come up with new standards for AI safety and security." That's not a bad thing. We're not going to get it right on the first try, but at least even thinking about this and raising awareness around it and challenging the agencies to basically stand up to some kind of standard and accountability. That's a very good thing.

The section on protecting American privacy is also very good because it actually brings in issues of when do we transgress, what is OK, and what is not. It makes a valid topic of discussion, that the government cannot just go about it without thinking about the consequences.

Advancing equity and civil rights check the box in terms of sensitizing everyone to the fact that these algorithms could be used for their own purposes.

The parts that have to do with promoting research and promoting understanding and promoting accessibility that can be positive as well.

Where do you think the directive falls short?

It fell short in actually spelling out actual numbers. Nothing could stop the White House from saying, "We want to see at least, I don't know, some number—5%, 10%, 20%—some number of resources dedicated to

this area." That becomes very meaningful. You can easily issue something that says, "I want to see at least 5% of the resources spent by this government agency or by every government agency into this category" as an example.

Another area where it fell short is spelling out in more details about how each agency should go about showing that it is responsive to the directive. At least have a list saying, "Here are some key performance indicators we are going to measure you by."

The last part is the budget. There should have been a part that says, "Here is some guidance for how much of the budget should be going to these areas." Because, at the end of the day, if you don't dedicate a budget to it, you're not really doing much. I think this directive, while good on a political front and good on a general public awareness front, doesn't have those teeth that actually enforce action. They're more like guidelines.

How enforceable is this executive order?

That's a great question because it's not clear. In a sense, the government agencies report to the executive branch and the head of the executive branch is in the White House. When the White House indicates that these are areas they want the agencies to pay attention to, they are supposed to heed it. However, how this translates into budgets, redirecting priorities into making decisions, that's where the rubber hits the road. That's where these set of directives are silent.

We all know the devil is in the details. You could always say you want to do this good (deed) or that good (deed), but if you don't translate that into budgets and programs and truly sacrifice in favor of other areas, then it's going to be very hard to guess what the outcome is.

Will this retroactively apply to AI technologies already out in the wild?

The scope as stated impacts anything that is already implemented, under development and will be developed. Now again, can we make that more perspective around what the agency should be doing and how much resources they should be committing or decommitting from other areas? That is what is sorely missing here.

It's not enough to say, "This area is very important. We can't afford to fall behind and we care about it being developed the correct way." It's also very important to say, "Here's how we are actually reallocating budgets, or we are creating new programs, and we are funding new programs."

What do you make of the fact that Biden created all these new AI rules through an executive order as opposed to going through Congress?

The executive order is not going to hurt. It's probably a necessary step to prepare and bring attention to Congress to do this. As you bring up these issues to federal agencies, you're basically telling them, "The White House is looking at these issues. We are paying attention. And we care about these aspects." One of the worries I have is agencies have a huge variance about how much they care about this or not.

Is this going to help with legislation? I think certainly because as the agencies begin to consider these things and highlight these issues that's going to be a forcing function for Congress to basically say, "OK, now it's time for us to pay attention and try and clarify what must be done, where the limits are, what should governed and what should be regulated."