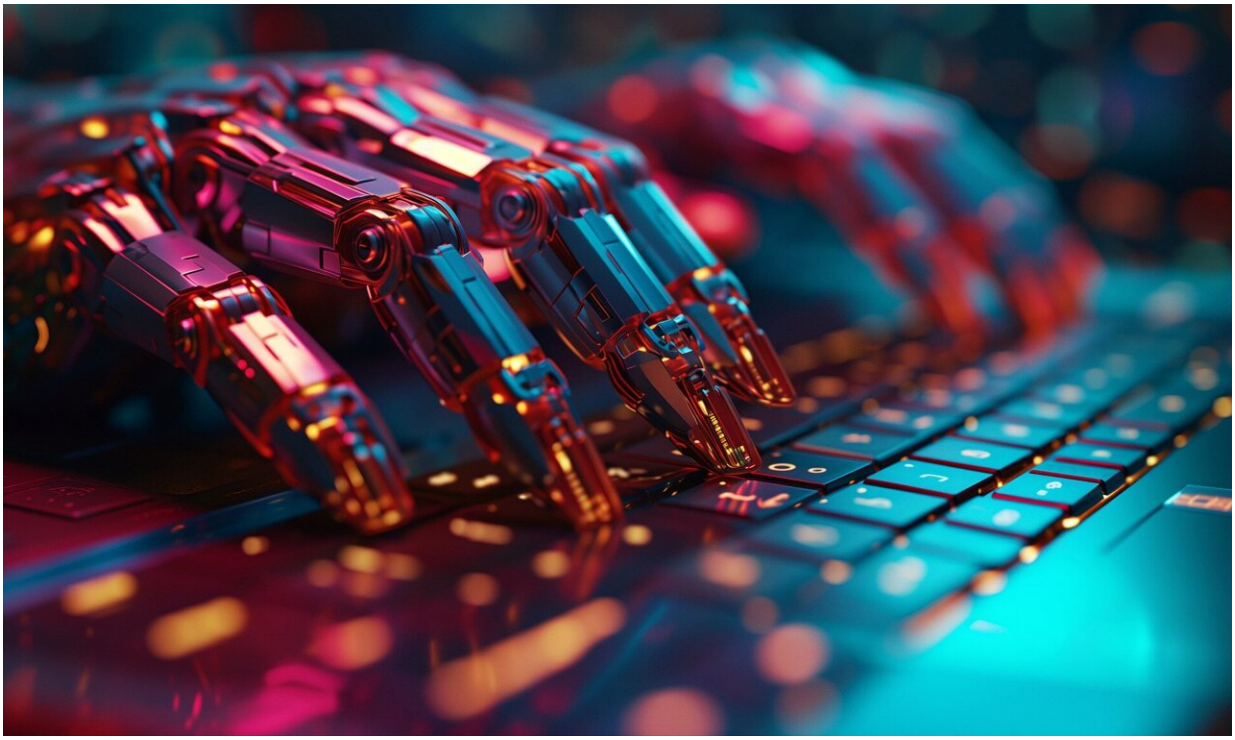
The challenges of regulating artificial intelligence

January 12 2024



Credit: Pixabay/CC0 Public Domain

In 1950, Alan Turing asked, "Can machines think?" More than 70 years later, advancements in artificial intelligence are creating exciting possibilities and questions about its potential pitfalls.

A recent executive order issued by President Joe Biden seeks to establish

"new standards for AI safety and security" while addressing consumer privacy concerns and promoting innovation. Georgia Tech experts have examined the key elements of the order and offer their thoughts on its scope and what comes next.

A precautionary tale

The order calls for the development of standards, tools, and tests to ensure the safe use of AI. From voice scams and phishing campaigns to larger-scale threats, the technology's potential dangers have been widely documented. But Margaret Kosal, associate professor in the Ivan Allen College of Liberal Arts, says that additional context is often needed to dispel hysteria.

"No one is going to be hooking up AI to launch nuclear weapons, but AI capabilities may enable targeting, or enable the command and control and the decision-making time to be compressed," she said.

The order will create an AI Safety and Security Board tasked with addressing critical threats. Companies developing foundation models that "pose a serious risk to national security, national economic security, or national public health and safety" will be required to notify the federal government when training the model and required to share the results of all red-team safety tests—a simulated cyberattack to test a system's defenses.

Since the launch of ChatGPT in 2022, a CNBC report details a 1,267% rise in phishing emails. Srijan Kumar, assistant professor in the College of Computing, attributes the increase to the technology's availability and an inability to rein in "bad actors."

He says these scams will only continue to get more sophisticated and personalized. They "can be created by knowing what you might be

willing to fall prey to versus what I might fall prey to," said Kumar, whose systems have influenced misinformation detection on sites like X (formerly Twitter) and Wikipedia. "AI is not going to autonomously do all of those bad things, but this order can ensure there are consequences for people who misuse it."

A delicate balance

Building an AI platform requires large amounts of data regardless of its intended application. Two primary goals of the executive order are protecting privacy and advancing equity.

To protect personal data, the order tasks Congress with evaluating how agencies collect and use commercially available information and address algorithmic discrimination.

Acknowledging that everyone should be allowed to have their voice represented in the outputs of AI data sets, Deven Desai, associate professor in the Scheller College of Business, noted, "There are people who don't want to be part of data sets, which is their right, but this means their voices won't be reflected in the outputs."

The order also includes sections to address intellectual property concerns among inventors and creators, though legal challenges will likely set new precedents in the years ahead.

When that time comes, Kosal says that defining "theft" in the context of AI becomes the true challenge and that, ultimately, money will play a significant role. "If you spit out a Harry Potter book and read it yourself, nobody will care. It's when you start selling it to make money, and you don't share proceeds with the original people, then it becomes an issue," she said.

What does AI-generated mean?

The order instructs the Department of Commerce to develop guidelines for content authentication and watermarking to label AI-generated content. Desai questions what it means for something to be truly created by AI.

An important distinction lies between using AI to assist a writer in organizing their thoughts and using the technology to generate content. He likens the trend to the music industry in the 1980s.

"Synthesizers really changed people's ability to generate music and, for a while, people thought that was horrible. They can just program the music. They're not. I am still the human responsible for that music, or that article in this case, so what is the point of the label?" he asks.

As AI assistance becomes commonplace in content creation, trusting the source of information is increasingly important. Recently, articles published on Sports Illustrated's website featured AI-generated content provided by a third-party company that had used a machine to write the content and create fake bylines. Sports Illustrated, which may not have known of the problem, ran the material without disclosure to readers. CEO Ross Levinsohn was ousted shortly after the story broke.

"Perhaps if the third party had disclosed its use of AI software, SI would have been able to assess how much AI was used and then chosen not to run the material, or to run it with a disclaimer that AI helped write the material," Desai said. "Of course, even if they label the content as AI-generated, a reader still won't know exactly how much of the content came from AI or a human."

AI and the workforce

As AI systems and models become more sophisticated, workers may become more concerned about being replaced. To counteract these concerns, the order calls for a study to examine AI's potential impact on labor markets and investments in workforce training efforts.

Kumar compares the rise of AI to similar technological innovations throughout history and sees it as an opportunity for workers and industries to adapt. "It's less a matter of AI replacing workers and more of reskilling people to use the new technology. It's no different from when assembly lines in the auto industry were created."

Promoting innovation and competition

The power to harness the full potential of AI has initiated a race to the top. Desai believes that part of the executive order providing resources to smaller developers can help level the playing field.

"There is a possibility here for markets to open up. Current players using models that weren't built with transparency in mind might struggle, but maybe that's OK."

The issue of reliability and transparency comes into focus for Desai, especially as it relates to government usage of AI. The order calls on agencies to "acquire specified AI products and services faster, more cheaply, and more effectively through more rapid and efficient contracting."

When taxpayer dollars are at stake, government can't afford to trust a technology it doesn't fully understand—a topic Desai has explored elsewhere. "You can't just say, 'We don't know how it works, but we trust it.' That's not going to work. So that's where there may be a slowdown in the government's ability to use private sector software if they can't explain how the thing works and to show that it doesn't have

discriminatory issues."

What's next

Promoting and policing the safe use of AI cannot be done independently. Georgia Tech experts agree that participation on a global scale is necessary. To that end, the European Union will unveil its comprehensive EU AI Act, which includes a similar framework to the president's executive order.

Due to the evolving nature of AI, the executive order or the EU's actions will not be all-encompassing. Law often lags behind technology, but Kosal points out that it's crucial to think beyond what currently exists when crafting policy.

Experts also agree that AI cannot be regulated or governed through a single document and that this order is likely the first in a series of policymaking moves. Kosal sees tremendous opportunity with the innovation surrounding AI but hopes the growing fear of its rise does not usher in another AI winter, in which interest and research funding fade.

Provided by Georgia Institute of Technology