With Executive Order, White House Tries to Balance A.I.'s Potential and Peril

President Biden announced regulations on Monday that seemed to have a little bit for everyone.

By Kevin Roose
New York Times

How do you regulate something that has the potential to both help and harm people, that touches every sector of the economy and that is changing so quickly even the experts can't keep up?

That has been the main challenge for governments when it comes to artificial intelligence.

Regulate A.I. too slowly and you might miss out on the chance to prevent potential hazards and dangerous misuses of the technology.

React too quickly and you risk writing bad or harmful rules, stifling innovation or ending up in a position like the European Union's. It first released its A.I. Act in 2021, just before a wave of new generative A.I. tools arrived, rendering much of the act obsolete. (The proposal, which has not yet been made law, was subsequently rewritten to shoehorn in some of the new tech, but it's still a bit awkward.)

On Monday, the White House announced its own attempt to govern the fast-moving world of A.I. with a sweeping executive order that imposes new rules on companies and directs a host of federal agencies to begin putting guardrails around the technology.

The Biden administration, like other governments, has been under pressure to do something about the technology since late last year, when ChatGPT and other generative A.I. apps burst into public consciousness. A.I. companies have been sending executives to testify in front of Congress and briefing lawmakers on the technology's promise and pitfalls, while activist groups have urged the federal government to crack down on A.I.'s dangerous uses, such as making new cyberweapons and creating misleading deepfakes.

In addition, a cultural battle has broken out in Silicon Valley, as some researchers and experts urge the A.I. industry to slow down, and others push for its full-throttle acceleration.

President Biden's executive order tries to chart a middle path — allowing A.I. development to continue largely undisturbed while putting some modest rules in place,

and signaling that the federal government intends to keep a close eye on the A.I. industry in the coming years. In contrast to social media, a technology that was allowed to grow unimpeded for more than a decade before regulators showed any interest in it, it shows that the Biden administration has no intent of letting A.I. fly under the radar.

The full executive order, which is more than 100 pages, appears to have a little something in it for almost everyone.

The most worried A.I. safety advocates — like those who signed an open letter this year claiming that A.I. poses a "risk of extinction" akin to pandemics and nuclear weapons — will be happy that the order imposes new requirements on the companies that build powerful A.I. systems.

In particular, companies that make the largest A.I. systems will be required to notify the government and share the results of their safety testing before releasing their models to the public.

These reporting requirements will apply to models above a certain threshold of computing power — more than 100 septillion integer or floating-point operations, if you're curious — that will most likely include next-generation models developed by OpenAI, Google and other large companies developing A.I. technology.

These requirements will be enforced through the Defense Production Act, a 1950 law that gives the president broad authority to compel U.S. companies to support efforts deemed important for national security. That could give the rules teeth that the administration's earlier, voluntary A.I. commitments lacked.

In addition, the order will require cloud providers that rent computers to A.I. developers — a list that includes Microsoft, Google and Amazon — to tell the government about their foreign customers. And it instructs the National Institute of Standards and Technology to come up with standardized tests to measure the performance and safety of A.I. models.

The executive order also contains some provisions that will please the A.I. ethics crowd — a group of activists and researchers who worry about near-term harms from A.I., such as bias and discrimination, and who think that long-term fears of A.I. extinction are overblown.

In particular, the order directs federal agencies to take steps to prevent A.I. algorithms from being used to exacerbate discrimination in housing, federal benefits programs and the criminal justice system. And it directs the Commerce Department to come up with guidance for watermarking A.I.-generated content, which could help crack down on the spread of A.I.-generated misinformation.

And what do A.I. companies, the targets of these rules, think of them? Several executives I spoke to on Monday seemed relieved that the White House's order stopped short of requiring them to register for a license in order to train large A.I. models, a proposed

move that some in the industry had criticized as draconian. It will also not require them to pull any of their current products off the market, or force them to disclose the kinds of information they have been seeking to keep private, such as the size of their models and the methods used to train them.

It also doesn't try to curb the use of copyrighted data in training A.I. models — a common practice that has come under attack from artists and other creative workers in recent months and is being litigated in the courts.

And tech companies will benefit from the order's attempts to loosen immigration restrictions and streamline the visa process for workers with specialized expertise in A.I. as part of a national "A.I. talent surge."

Not everyone will be thrilled, of course. Hard-line safety activists may wish that the White House had placed stricter limits around the use of large A.I. models, or that it had blocked the development of open-source models, whose code can be freely downloaded and used by anyone. And some gung-ho A.I. boosters may be upset that the government is doing anything at all to limit the development of a technology they consider mostly good.

But the executive order seems to strike a careful balance between pragmatism and caution, and in the absence of congressional action to pass comprehensive A.I. regulations into law, it seems like the clearest guardrails we're likely to get for the foreseeable future.

There will be other attempts to regulate A.I. — most notably in the European Union, where the A.I. Act could become law as soon as next year, and in Britain, where a summit of global leaders this week is expected to produce new efforts to rein in A.I. development.

The White House's executive order is a signal that it intends to move fast. The question, as always, is whether A.I. itself will move faster.