

Governments Setting Limits on AI

Many countries/regions are considering, or trying to implement, regulations on the training and use of artificial intelligence.

THE ISSUE OF setting limits on artificial intelligence (AI) varies by country, and with ChatGPT permeating seemingly all aspects of work and life, the U.S. government has finally begun implementing steps regulating its use.

In late October, President Joe Biden signed an executive order (EO) mandating that developers of AI systems that could pose risks to U.S. national security, the economy, public health, or safety share the results of safety tests with the U.S. government, in line with the Defense Production Act, before they are made public. The order also requires standards, tools, and tests to be developed to ensure AI systems are safe, secure, and trustworthy.

Further, the order calls on the Commerce Department to develop guidance for content authentication and watermarking, to clearly label AI-generated content to protect Americans from AI-enabled fraud and deception.

The EO calls for safeguards to protect Americans' privacy, address algorithmic discrimination, and other measures.

Here is a look at efforts under way to develop frameworks and guardrails for regulating AI around the world.

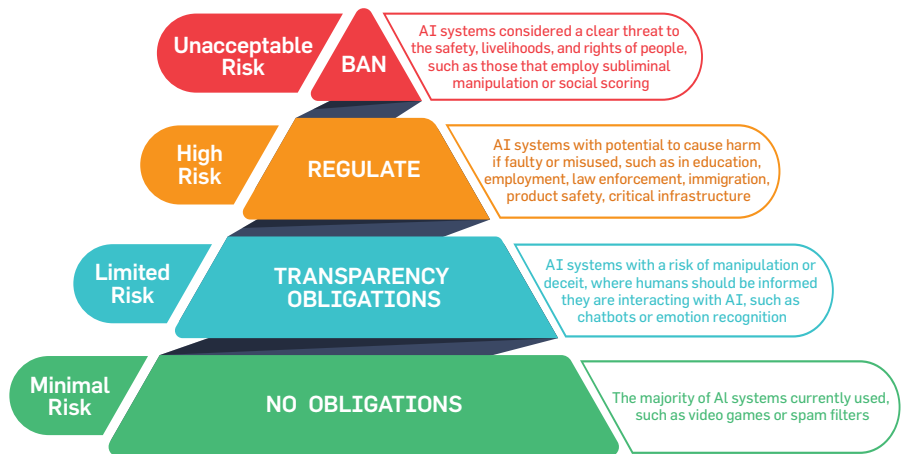
Classifying AI Risk in the E.U.

The Biden Administration's actions came on the heels of the European Union, which last June passed the landmark Artificial Intelligence Act, moving a step closer to formally adopting a first-of-its-kind set of comprehensive rules around regulating AI.

The AI Act, expected to be adopted early this year, sets four classifications for AI risk, ranging from minimal to unacceptable. Technology classified as an unacceptable risk, for example, would include systems that judge people based on a behavior known as social scoring, along with predictive policing tools, and would be banned.

The new E.U. regulations mandate

European Union Artificial Intelligence Act The Four Levels of Risk in AI



stronger privacy standards, stricter transparency laws, and steep non-compliance penalties with fines of up to €30 million (nearly \$33 million), or 6% of global income. There also will be an EU AI board to oversee the implementation and uniform application of the regulations, which will build on existing GDPR and Intellectual Property legislation.

The AI Act “is the first comprehensive regulation addressing the risks of artificial intelligence through a set of obligations and requirements that intend to safeguard the health, safety and fundamental rights of E.U. citizens and beyond, and is expected to have an outsized impact on AI governance worldwide,” wrote Mia Hoffmann, a research fellow at the Center for Security and Emerging Technology (CSET) at Georgetown University.

AI experts say other regions need to enact legislation to protect citizens in areas including privacy, security, and bias. “We need as much innovation in governance and risk mitigation as we need in development and deployment,” says Beena Ammanath, managing director of Deloitte Consulting and leader of its technology trust ethics practice.

She predicts that in the months and years ahead, AI regulations and laws will proliferate, propelled in part by growing industry calls to regulate generative AI.

“Industries where companies are already self-regulating are positioned to help shape rulemaking,” Ammanath says. “Regulators cannot inspect, at a technical level, all of the AI applications that are emerging across industries, particularly as innovation and deployment are occurring at such a rapid pace. When regulators consider how to develop rules that guide AI in the marketplace, they will likely look to known harms, as well as to known remedies and preventative measures.”

European Countries, Brazil Set AI regulations

In a move viewed as accelerating European AI regulations, France, Germany, and Italy have agreed to “mandatory self-regulation through codes of conduct,” according to Reuters, which reported seeing a jointly written paper.

Developers of machine learning foundation models of AI would be required to provide information about their models. While there are no sanc-

tions specified in the paper, they could eventually be set up.

Similar to the E.U., Brazil has developed a framework to categorize AI tools and their uses and ban those whose risk is found to be excessive, according to a bill that also establishes a new regulatory body to enforce the law. The legislation also introduces a protective system of civil liability for providers or operators of AI systems, along with a reporting obligation for significant security incidents, according to global tech advisory firm Access Partnership.

Regulating AI in the U.S.

In addition to the Biden EO, two frameworks have also been released, but neither is binding. One is the Blueprint for an AI Bill of Rights, released by the White House, which lays out the requirements we might want to demand of AI systems, notes Helen Toner, director of strategy and foundational research grants at CSET.

The AI Bill of Rights lays out five principles to guide the design, use, and deployment of automated systems to protect the American public. They are:

- Safe and effective systems—that undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring—that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards.

- Algorithmic discrimination protections—for when automated systems contribute to unjustified treatment or impacts disfavoring people based on race, color, ethnicity, sex, religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law.

- Data privacy—through design choices that ensure such protections are included by default, including ensuring data collection conforms to reasonable expectations and that only data necessary for the specific context is collected.

- Notice and explanation—system designers of automated systems should provide plain-language documentation, including clear descriptions of their function and the role automation plays.

- Human alternatives, consideration,

“AI is a general-purpose technology that can be used for many things, and... we wouldn’t expect to legislate everything in one bill.”

and fallback—the ability to opt out of automated systems in favor of a human alternative, where appropriate.

The framework, the National Institute of Science and Technology’s AI Risk Management Framework, was designed in collaboration with the private and public sectors and is meant to be a resource for companies building AI systems, Toner says. Its focus is on improving “the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.”

There are also multiple senators working on various AI legislation. Senate Majority Leader Chuck Schumer (D-NY) is working with a bipartisan group of senators to put together a relevant piece of legislation. Schumer told National Public Radio that AI needs to be regulated, and “if we don’t do something about AI, much worse things could happen.”

Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO) developed a bipartisan legislative framework as guardrails for AI. The framework includes establishing an independent oversight body, ensuring legal accountability for harm, defending national security, promoting transparency, and protecting consumers and children.

All of this means the likelihood of some sort of AI legislation emerging is pretty high, Toner says. “The big stumbling block is when policymakers think they have to solve all issues in one go,” she notes. “AI is a general-purpose technology that can be used for many things and ... we wouldn’t expect to legislate everything in one bill.”

Canada’s Voluntary Code of AI Conduct

Canada released a Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems that identifies measures organizations are encouraged to abide by in the development and management of generative AI systems.

The Canadian government introduced the Artificial Intelligence and Data Act in June 2022, and the Code is seen as “a critical bridge between now and when that legislation would be coming into force,” said Francois-Philippe Champagne, minister of innovation, science, and industry, in a statement.

Meanwhile, leaders of the G7, which includes Canada, France, Germany, Italy, Japan, the U.K., and the U.S., have agreed on a set of international guiding principles for regulating AI, and on a voluntary code of conduct for AI developers. The 11-point code “aims to promote safe, secure, and trustworthy AI worldwide and its purpose is to provide voluntary guidance for actions by organizations developing the most advanced AI systems, including the most advanced foundation models and generative AI systems,” the G7 document said.

China: Three Sets of AI Regulations

The Cyberspace Administration of China has released three sets of regulations tied to AI. The first targets algorithmic recommender systems, which recommend products you may want to buy or videos you may want to watch. Toner called that “an interesting piece of legislation,” noting that recommendation systems tend to be “boring” and not as interesting as self-driving cars, although they are much more widespread.

This also appears to be in contradiction with Article 8 of the new draft regulations, which prohibits apps from advertising their users, Toner notes.

There are also rules for synthetically generated content and the use of generative AI. “The draft generative AI regulation requires both the training data and model outputs to be ‘true and accurate,’ a potentially insurmountable hurdle for AI chatbots to clear,” wrote Matt Sheehan in a Carnegie Endowment for International Peace blog.

All three regulations require develop-

ers to file with China's new algorithm repository, which gathers information on how algorithms are trained, along with requiring them to pass a security self-assessment, Sheehan noted.

Toner says there have been rumors China wants to develop a comprehensive law to cover all types of AI.

Africa: Slow AI Adoption

AI regulation may be a long time in coming to Africa, as the AI landscape there is "quite fragmented," with "different perspectives and policies across African countries," says Conrad Tucker, interim director of CMU-Africa and associate dean for international affairs-Africa at Carnegie Mellon University.

As a whole, Africa has been slow to adopt AI technologies. The Global AI Index characterizes Egypt, Nigeria, and Kenya as "nascent," and Morocco, South Africa, and Tunisia as "waking up," to AI.

The Centre for Africa-Europe Relations argued that "African countries should not prioritize adopting AI-specific laws, but instead focus on strengthening the foundational requirements on data governance. If properly done, the implementation and enforcement of data protection laws is the first step in the journey toward AI regulation."

So far, Mauritius has published a national AI strategy—reportedly the first African country to do so. Egypt launched its AI strategy in 2021, while Kenya has formed an AI task force to create guidance on how AI technologies can help further the country's development, according to *TechCabal*, a self-described "future-focused publication that speaks to African innovation and technology in depth." Rwanda has created a technology center of excellence whose work includes development of an AI strategy. Nigeria has not formulated a national policy on AI, but it has a National Center for Artificial Intelligence and Robots, the site reported.

It behooves Africa to deepen its use of AI technologies to transform its economy. The elements are there: it has a young, curious, tech-savvy, and entrepreneurial population that is increasingly educated, according to the Africa Regional Science, Technology and Innovation Forum (ARSTI2021) report assembled by the United Nations Economic Commission for Africa.

Making the Case for Legislating AI

As chair of ACM's global Technology Policy Council, Jim Hendler says regulating AI should be explored. Speaking personally, it is necessary, says Hendler, who is also an AI researcher and computer, Web, and cognitive professor at Rensselaer Polytechnic Institute (RPI).

Observing that social media was not regulated in its early days, when it would have been easier to incorporate privacy controls, he says the same thing could happen with AI, especially as generative AI tools are getting easier to use. This is creating issues with misinformation and disinformation, Hendler says.

As an example, he points to a video released several months ago showing a bombing at the Pentagon; the stock market dropped in response, until it was revealed the video was a generative AI fake.


"Here's the thing: No one actually broke a law, unless it was specifically done to [tank] the stock market," Hendler says. This makes it critical to tag anything that is AI-generated, he says, "So you could have a law saying removing such a tag would be illegal now," with the potential for fines to be levied.

Facial recognition is another area that has some benign use cases with no serious implications, but there are others that could lead to misuse and a person's loss of liberty if they were to be misidentified, Hendler says. An AI system used to identify passengers at airports is very different than using such a system to observe a demonstration in the streets and trying to identify people who are there, he notes.

Hendler believes the ideal legislation would include provisions for algorithmic transparency and watermarks. He expects we will start seeing "piece-wise regulation" put forth by states, agencies, and different industries, adding that it is unlikely a single agency devoted to regulating AI will be created because "the argument is, why would you expect rules that apply to automobiles to be the same as the ones for pacemakers?"

Deloitte surveys indicate "Organizations are supportive of government playing a role in technology regulation," says Ammanath, specifically

in fostering cross-business collaboration to define standards (69%), setting regulations (59%), incentivizing adoption of standards (50%), and imposing financial penalties (37%).

In terms of what the future holds, there is general agreement that AI should be regulated, even though approaches differ vastly from comprehensive legislation to those aimed at specific use cases and voluntary guidelines. To help stay abreast of ever-changing updates in individual jurisdictions, the non-profit International Association of Privacy Professionals (IAPP) has developed a Global AI Legislation Tracker, a live repository of more than 1,000 AI policy initiatives from 69 countries and the AU. The center said its other motive is to help organizations create trustworthy AI governance systems—an admirable goal, given that use of AI is seemingly ubiquitous. 

Further Reading

Hauptfleisch, W.
"Where the world is on AI regulation."
October 2023. *Medium*.
<https://bit.ly/49obPaT>

Hoffmann, M.
The EU AI Act: A Primer. Center for Security and Emerging Technology. September 2023.
<https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/>

Looking into the crystal ball: Artificial intelligence policy and regulation in Africa. The Centre for Africa-Europe Relations. September 2023. <https://bit.ly/42NCK72>

BSA Analysis: State AI Legislation Surges by 440% in 2023. BSA/The Software Alliance. September 2023. <https://bit.ly/3T6xK0x>

Zhu, K.
The State of State AI Laws: 2023. Electronic Privacy Information Center. <https://epic.org/the-state-of-state-ai-laws-2023/>

EU AI Act: First regulation on artificial intelligence, European Parliament. August 2023. <https://bit.ly/3uOh8RF>

Sheehan, M.
China's AI Regulations and How They Got Made. July 2023. Carnegie Endowment For International Peace. <https://bit.ly/3I4eSjg>

"Artificial intelligence in Africa: National strategies and initiatives." *Diplomacy*. <https://bit.ly/4bMTqpS>

Esther Shein is a freelance technology and business writer based in the Boston, MA, USA, area.