

AI Around the Globe: What to Know in 2024

Wiley Connected

January 3, 2024

In this Wiley Connected podcast, hear from Wiley Partners Amb. David Gross, Duane Pozza, Joan Stewart, and Consulting Counsel Jacqueline Ruff about the latest in international developments surrounding Artificial Intelligence (AI). The topics discussed include the Biden Administration AI Executive Order (EO), the role of the Organization for Economic Cooperation and Development (OECD) and the United Nations (UN) regarding AI, and the EU's landmark AI Act.

Transcript

Intro

You're listening to Wiley Connected. A series of podcasts on tech, law, and policy. In each podcast technology focused lawyers at Wiley, a Washington, D.C. law firm, break down innovation and law with a uniquely D.C. perspective.

David Gross

Hello. Welcome. My name is David Gross and I'm a partner at Wiley and part of Wiley's preeminent TMT practice. I am joined today by three of my great colleagues who, like many others at Wiley, are expert on virtually all legal aspects of AI. During today's podcast, Duane Pozza will discuss the recently released Biden Administration AI executive order. Then Jackie Ruff will discuss the role of the OECD and the United Nations regarding AI, and then Joan Stewart will discuss the EU's new, about to be adopted, AI Act. Duane, can you start us off?

Related Professionals

Amb. David A. Gross
Senior Counsel
202.719.7414
dgross@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

AI Executive Order
Artificial Intelligence (AI)
Federal Policy and Regulation
GDPR and Global Privacy
Privacy, Cyber & Data Governance
Telecom, Media & Technology

Duane Pozza

Thanks, David. So, I want to start off today by talking about the White House executive order for safe, secure, and trustworthy artificial intelligence, generally known as the AIEO. It was released on October 30th, 2023, and it outlines a sweeping plan for encouraging the development and managing the risks of AI. It's notably lengthy, it includes dozens of directives to numerous agencies throughout the federal government that will be implemented over the next year. We actually have our own tracker we've developed on the EO that is over twenty-six pages long and it continues to grow.

So, these directives are wide ranging and they will generally impact companies that are developing and deploying AI. There are some directives to the private sector. There are some new requirements for government contractors and significant work on new AI standards, guidance and best practices that we will expect will be used by the private sector.

There's also a clear determination to lead internationally and work with other countries and European Union on these standards and the overall approach. So at a high level, the EO's directives fall under eight guiding principles and priorities. These include ensuring safety and security, promoting innovation and competition, advancing equity and civil rights, and protecting privacy and civil liberties.

Notably, there are areas where a regulatory approach by the U.S. and thinking about how other countries will view AI, is potentially on the table and two key decision points going forward under the EO are the extent to which AI will be regulated along the lines of these principles that are outlined in the EO and then also whether or not there will be harmonization between different countries and jurisdictions and their approach on these issues and I think this is particularly important because AI development and use crosses borders and includes models that are trained on data that crosses borders and it's often difficult to have large AI models that can function with different kinds of regulatory structures around them.

So I just want to briefly highlight a few of the focuses of the EO. One major focus is AI safety, which is consistent with an issue that is getting a lot of attention internationally particularly in the E.U. and particularly the safety of large general purpose models often called foundation models is an issue. These are models that can be used for a variety of purposes and a variety of different use cases by the private sector and the public sector. This concern with AI safety is spurred largely by these generative AI models that can generate content, but the definition is not limited to just generative AI. So, as an example, the EO reports to direct directly regulate under the Defense Production Act, the reporting of certain safety features of these foundation models by requiring reporting to the Department of Commerce.

Additionally, another part of the Department of Commerce, NIST, is developing standards for red teaming, basically a way of testing the safety and security of these models. And also, CISA, which is in DHS, it's the Cybersecurity and Infrastructure Security Agency is looking into AI as it is used in critical infrastructure. It's already working with the U.K. and announcing guidance on how AI can be safely implemented as part of critical infrastructure.

A second large focus is on rights impacting AI. This covers things like dangers with potential bias, accuracy, and ensuring human review and input in AI decisions. So the EO has specific directives to agencies like Homeland Security and the Department of Justice on enforcing their own non-discrimination laws and separately, an EO seeks to use the levers of agency use and procurement of AI to require risk assessments to deal with these issues, like bias, accuracy and human review, in a way that will flow down to private sector, in particular, those that deal with the government. And the last piece I want to highlight is there's an element of improving American competitiveness on AI. There are initiatives to promote AI talent including within federal agencies. There is a focus on the semiconductor industry as being critical to AI developments, including an instruction to the Secretary of Commerce to utilize the Chips Act to provide more opportunities to startups and small businesses.

It's also important to realize that much of this work that I've just outlined is being done domestically is meant to feed into an international approach under the EO. The EO suggests the U.S. has the opportunity to work with international allies and partners to lead the way on AI policy and to establish international standards for AI to promote these principles.

So, there's a few notable components I'll outline. There's a focus on engagement with international allies and partners. So the Secretary of State and others at the Administration are tasked with expanding engagement with allies and partners to provide updates on AI policy and establish an international framework to address the risk benefits of AI. The Secretary of State is responsible for establishing a plan for global engagement in AI policy which will be guided in part by risk management frameworks that are already being developed domestically, including by NIST at the Department of Commerce. Secretaries of State and Commerce acting through NIST are to publish an AI and global development playbook that incorporates the RMF's principles, guidelines, and best practices and the Secretary of State is to establish a global AI research agenda and finally, for this purpose, there's coordination on critical infrastructure safety. The Secretary of Homeland Security and Secretary of State are to develop a plan that encourages international adoption of AI safety and security guidelines for critical infrastructure.

So note these, this is an ambitious agenda, and it's also an ambitious timeline. The directives in the EO are meant to come into place and be fulfilled over the next year. So there'll be much to watch and many more updates to come as the different directives for the EO roll out. With that, I will turn it over to Jackie to talk a bit more about what's happening on the international stage.

Jackie Ruff

Thank you, Duane, for that very complete description of the highlights on the EO and especially the international portions, which are relevant to what I'm going to talk about now.

During this period of escalating calls for AI policy and regulation, international organizations are working hard on frameworks with implications for businesses. These include whether there will be mandatory rules, what types of businesses and AI functions will be covered, and how accountability for private sector will work. Two important venues as David mentioned at the outset, one is the OECD, the Organization for Economic

Cooperation and Development. This is an organization of thirty-eight member countries with participation by the European Commission and additional country observers. The OECD adopted the very first set of ethical AI principles in 2019 and worked very closely with Europe on theirs. The OECD work on AI has grown dramatically and been followed around the world.

Recently, the OECD updated its definition of AI and to better encompass generative AI to clearly cover the entire life cycle of AI from system design through use. It has also worked on ensuring accountability for businesses through what are called Responsible Business Conduct Practices, RBC practices.

Businesses frequently have set these up for other reasons, such as human rights impact assessments and transparency reports. To encourage innovation the OECD has promoted the idea of sandboxes in which businesses can test AI in a flexible regulatory environment. Watch for a robust OECD work program in 2024. Close collaboration with the European Commission and the G7, and policy collaboration through active international engagement and cooperation, such as Duane was describing.

Secondly, AI is a major focus at the United Nations. Some might say the U.N. is not going to regulate my business, it does not have direct authority over my business, and it moves too slowly to matter. Often a valid comment about the U.N. but as countries around the world try to regulate the sweeping expansion of AI they will look to the U.N. for models. The U.N. Secretary General has led an initiative to develop global digital policy since 2018. Under the heading of digital cooperation his office has produced papers and general guidance related to AI and recently created a high level AI expert advisory group.

Most importantly, AI will be included in a planned global digital compact. That is a set of commitments by U.N. members to be adopted at a summit on the future next September and as it happens in July, UNESCO, the U.N. agency, adopted global standards for AI ethics, including a model impact assessment and guidance for audits and due diligence.

This UNESCO framework has been promoted for inclusion in the global digital compact. So there is already a model out there for those who look for it, whether it national, or regional, or global purposes. Developments like these raise the prospect of new and divergent regulations that will impact U.S. based businesses in markets around the world. Understanding the OECD and the U.N. approaches and expectations of the private sector could be relevant for business planning and risk management for businesses of all types throughout the AI lifecycle. There are many ways for businesses to provide input to these intergovernmental processes by engaging for governments. For example, by working through the executive orders activities by the Department of State and Commerce. This is a place for monitoring, for advocacy, and one of many such opportunities that are only going to increase next year to shape policies relevant to business. And with this, I'd like to turn to Joan to talk about the EU AI Act, a key focus necessarily at this time.

Joan Stewart

Thanks so much, Jackie. So, there were exciting developments at the end of 2023, signaling that the EU's AI Act will get across the finish line before the EU parliamentary elections in 2024.

So after a marathon session of negotiations in early December, the European Commission, Council, and Parliament announced that they have reached a provisional agreement on the regulations around AI. So the AI Act is a wide ranging set of rules really relevant to anyone who is building a system that uses AI, that will be used by individuals in the EU, or to individuals located in the EU that are engaging with AI. Additionally, as it is one of the first comprehensive laws governing AI, it is expected that the AI Act will influence other laws globally that seek to regulate AI. So like the GDPR, the AI act is extra territorial, meaning that it can apply to organizations outside of the EU if you meet certain criteria. So based on current expectations, the AI act will be adopted by second quarter of 2024. The effective date of various provisions are staggered with the majority of the obligations taking effect about two years after the act is adopted.

So, how will the AI Act potentially impact your business? The Act adopt a risk based structure. AI systems are classified either as prohibited, high risk, limited risk, or minimal risk, and the compliance obligations are accordingly scaled based on that risk. So there are some exemptions for AI uses for national security, military and defense, some research and development, and some open source uses. If your business activities fall under that prohibited risk category, be prepared to stop those uses within six months of the act effective date. So these include activities like social credit scoring system, a motion recognition system, behavioral manipulation, untargeted scraping of facial images for facial recognition, among others.

High risk uses are the next step down the risk scale. These include uses related to medical devices, vehicles, recruitment, HR or worker management, influencing votes in elections, biometric identification, and critical infrastructure. Businesses that use AI systems for high risk uses will face significant compliance obligations, including a fundamental rights impact assessment requirement, registration with a public EU database, the obligation to engage outside audit and maintaining human oversight of the system.

Additionally, be prepared to build out significant internal compliance systems if you're using these high risk AI system. These include bias mitigation and significant security protocols, including testing and monitoring.

So, no AI system really gets off scot-free in the AI Act. The Act contains requirements for general purpose AI and foundation models as well and importantly, any system that uses generative AI must be transparent. These transparency requirements will take effect twelve months after the Act takes effect. All AI content must be labeled so users know they are interacting with generative AI content. Here clearly, the goal is to avoid deepfakes and the AI Act specifically imposes more stringent requirements depending on the strength of the AI model. Where the strongest models, like those developed by open AI, will have to be tested for vulnerabilities by third party organization. Similar to the GDPR, the enforcement mechanism in the AI Act is significant for prohibited AI violations fines can be up to seven percent of global annual turnover. Most other violations are capped at three percent of global annual turnover, which is still not an insignificant amount depending on the scope of your business. The bottom line here, any business that is building AI models or engaging with users in the EU using generative AI, should pay close attention to the AI Act and that really wraps up our discussion of the AI Act.

Duane Pozza

Thanks, Joan. One big takeaway from our discussion is that companies will need to watch developments in AI policy and regulation closely throughout 2024 on both the domestic and international level; and I think another big takeaway is that there will be opportunities for engagement on many of these policy initiatives, including many of those under the executive order I talked about earlier. So please do reach out to any of us if you're interested in further engaging or following AI developments in 2024 and thanks for listening.

Outro

Thank you for tuning in to the Wiley Connected podcast brought to you by the attorneys at Wiley. If you enjoyed this episode of Wiley Connected, we encourage you to subscribe, rate, and leave a review on iTunes and SoundCloud. For additional resources and materials, head over to wileyconnect.com. Thank you for listening.

The views, information, or opinions expressed during the series are solely those of the individuals involved and do not necessarily represent those of Wiley Rein LLP and its employees. The material contained in this podcast is not intended to be and is not considered to be legal advice. Transmission is not intended to create and receipt does not establish an attorney client relationship.