Export Compliance Manager

Regulating AI

Balancing innovation and national security

Reprinted with permission from the November 2023 issue of
Export Compliance Manager

www.exportcompliancemanager.com

Issue 38. NOVEMBER 2023

Regulating AI: balancing innovation and national security

The rapid expansion of artificial intelligence ("AI") will bring incredible advancements to science and industry and undoubtedly change our lives. For instance, AI has the potential to be a game changer in the medical field, especially in drug development and predicting disease risk. There is, however, growing concern over the widespread dangers posed by AI from work displacement, proliferation of false information, mass surveillance and the repression of vulnerable groups to the development of advanced autonomous AI weapons. Earlier this month, on 1 November 2023, the United States and 30 other nations announced a non-binding declaration to establish guidelines for the military use of AI.[1] Some autonomous weapon systems already exist and have been deployed, such as defensive systems that can shoot down incoming missiles. There are reports of lethal autonomous drones being developed for the Russian-Ukraine conflict.[2] Further, although AI could be used to strengthen cyber defenses by building more secure code and detecting threats, it could also drastically increase the lethality of cyber offensive weapons – potentially causing catastrophic harm. Accordingly, the United States is racing to advance its own AI technology while seeking to limit access to critical US technology, components, and advanced semi-conductors by its adversaries, primarily the People's Republic of China ("PRC").

What is AI? AI refers to machines that can learn from experience, adjust to new inputs, and perform human-like tasks by themselves. Over the last year, we have seen the rise of generative AI models. Generative AI consists of systems that can create new content such as images, videos, text, and audio from simple text prompts such as ChatGPT. This, however, only represents a small segment of how AI is currently being used. AI includes chatbots as well as deep-

> On 1 November 2023, the United States and 30 other nations announced a non-binding declaration to establish guidelines for the military use of AI.

learning and large language models that can mimic human neural networks, analyze massive volumes of data, and make decisions. Advanced AI systems raise significant national security concerns because they can be used to improve the speed and accuracy of military decision making and increase electronic warfare, radar, signals intelligence, and jamming capabilities.

Efforts to impose regulations on the development of AI

In recognition of the threats posed by AI, nations are proposing regulations or frameworks for its safe and secure development. On 30 October 2023, President Biden issued the first-ever AI executive order ("EO") on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This EO establishes sweeping directives and priorities across a wide swath of areas controlled by the federal government. Among other actions, the EO directs the following:

- Under the Defense Production Act, establish a requirement that developers of powerful AI systems share the results of all red-team safety tests and other critical information with the US government.
- The National Institute of Standards and Technology ("NIST") will develop industry standards and guidelines to ensure the development of safe, secure, and trustworthy AI systems.
- Federal agencies will evaluate the risks of AI being used to engineer dangerous biological weapons.
- The Department of Commerce ("DOC") will develop guidance for content authentication and watermarking to clearly label AI-generated content to prevent AI-enabled fraud and deception.
- The departments of Defense and Homeland Security will evaluate and assess AI risks to improve US cyber defenses and offensive capabilities and develop AI tools to find and fix vulnerabilities in critical software.

While this EO provides an important framework and identifies the national security threats, the US still lacks federal data privacy legislation to protect personal information. This is even more critical now as we are already seeing AI chatbots like WormGPT and FraudGPT being weaponized for malicious purposes to craft convincing phishing emails and create undetectable malware to launch cyberattacks.

The European Union will likely finalize its AI Act by the end of the year; it was first proposed in April 2021 but negotiations reportedly broke down on 10 November 2023 among disagreements regarding the regulation of foundation models such as Open AI's GPT-4 model and concerns that increased EU regulation in this area could negatively impact the EU with its US and Chinese competitors. The AI Act would regulate any AI systems that are "placed on the market, put into the services or used in the EU", based upon a risk-based approach. This Act would also ban any AI system that presents unacceptable risks. For instance, the EU intends to prohibit government social scoring tools, devices that employ cognitive behavioral manipulation techniques such as voice-activated toys that encourage dangerous behaviors and real-time, and remote biometric identification in public spaces such as live facial recognition systems. Other systems that raise high risks will be carefully monitored, but developers of AI systems will be self-assessing and self-certifying the risks associated with each system and whether it complies with requirements of the Act.[3]

Export control regulations applicable to AI

International Traffic in Arms Regulations ("ITAR")

Although the term "Artificial Intelligence" does not appear in the US Munitions List ("USML") that does not mean that defense articles that incorporate AI fall outside the ITAR's controls. For example, swarming capabilities used in unmanned aerial vehicles ("UAVs") to operate autonomously without human input to avoid collisions, adapt to changes in the threat environment, or fly in formations is possible due to AI tools. UAV flight control systems with threat-adaptive autonomous flight controls systems and those with swarming capabilities are both classified under Category VIII of the USML. Similarly, AI tools developed for electronic warfare systems, offensive cyberwarfare, radar, surveillance, counter-surveillance, autonomous underwater vehicles, and jamming are controlled under Category XI of the USML. Further, the Department of Defense ("DOD") is currently developing numerous weapons systems that use AI[4] and the results of any AI research project funded by DOD for military purposes would also be classified under the USML. Accordingly, defense contractors should ensure they they have adequate technology control plans and they safeguard all ITAR-controlled technical data properly to avoid the release of technical data to foreign persons (i.e., illegal exports) within the United States.[5]

Lastly, the ITAR prohibits US persons and companies from providing services to a foreign person to develop an AI-based weapon system or provide training on how to use AI to develop, manufacture, or produce military weapons such as a lethal autonomous weapon.[6]

Export Administration Regulations ("EAR")

In addition to controlling for export advanced computational devices – neural computers – that leverage machine learning to simulate the operations of a human brain to perform specific tasks under Export Control Classification Number ("ECCN") 4A004 of the Commerce Control List ("CCL"), beginning in October 2022, the Department of Commerce's Bureau of Industry and Security ("BIS") has imposed extensive regulations to restrict the PRC's access to US advanced semiconductors and semiconductor manufacturing equipment used to develop AI. On 17 October 2023, BIS issued further updates to these rules that go into effect on 17 November 2023 that set tighter restrictions on AI chips, strengthen restrictions on semiconductor equipment, and add more Chinese companies to the DOC's Entity's List. These new rules were designed to close loopholes that had allowed the PRC to obtain chips that were just below the restricted thresholds, which could provide AI model training very similar to the advanced chips BIS had banned for national security reasons. BIS has also expanded licensing requirements to more than 40 countries and requires companies to notify BIS of exports of certain chips with performance capabilities just below the restricted levels. The intention of these rules is clear – to stop the PRC's goal of overtaking the United States and its allies in the field of AI. Accordingly, BIS articulated that these new rules were designed to thwart "PRC's efforts to obtain semiconductor manufacturing equipment essential to producing advanced integrated circuits needed for the next generation of advanced weapon systems, as well as high-end advanced computing semiconductors necessary to enable the development and production of technologies such as artificial intelligence (AI) used in military applications."

The results of any AI research project funded by DOD for military purposes would also be classified under the USML.

Catch-all provisions

In addition to license requirements for items assigned a specific ECCN, export controls under the EAR are based upon the identity of the end-user, the location of the end-user, and the end-use. The EAR prohibits US persons (including US companies) from exporting and reexporting any US-origin items, software, or technology, without a license, to any destination (with limited specified exceptions) if they know that the item will be used directly or indirectly in the production, development, or use of missiles, chemical or biological weapons, or nuclear weapons.[7] Moreover, Section 744.6 of the EAR makes it unlawful for US persons to provide "support", without a license from the Department of Commerce, for the development, production, or use of weapons of mass destruction in specific countries (including the PRC), even if none of the underlying commodities, technologies, and software involved in the activity are subject to the EAR.

Conclusion

The US government is keenly aware of the dangers posed by AI and will continue to assess how best to protect its national security interests using export controls. The Department of Justice has indicated that it is especially concerned about nation-state adversaries such as the PRC, Iran, Russia, and North Korea obtaining advanced technologies like AI to enhance their military capabilities. It will undoubtedly use its whole-of-government approach and the resources of the Disruptive Technology Task Force to investigate and prosecute any illegal exports or schemes to evade US export laws that may result in our adversaries obtaining US components, software, or technology that could advance dangerous AI systems. As laws continue to expand in this area, a robust compliance program is critical! ■

About the author:

B. Stephanie Siegmann is a Partner at the law firm of Hinckley, Allen & Snyder LLP, and Chair of its International Trade and Global Security Practice.

www.hinckleyallen.com

1 "The US and 30 Other Nations Agree to Set Guardrails for Military AI," Wired, Nov. 14, 2023.
2 Id.
3 See The EU's AI Act, available at https://artificialintelligenceact.eu/the-act/.
4 See e.g., U.S. GAO Report to the U.S. Senate Committee on Armed Services, "Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions (June 2023).
5 See 22 C.F.R. § 120.56 (defining release of defense technical data); 22 C.F.R §127.1(a)(1) (it is unlawful "to export or attempt to export from the United States any defense article or technical data").
6 See 22 C.F.R. §120.32 (defining defense service).
7 See 15 C.F.R, §§ 744.2-744.4.