Shumaker

APRIL 17, 2020 | PUBLICATION

Client Alert: Export Controls in The Age of Artificial Intelligence: Is Your Company Compliant?

Download Client Alert: Export Controls in The Age of Artificial Intelligence: Is Your Company Compliant?

SERVICE LINE

Intellectual Property
Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Tom BenGera
Patrick B. Horne

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The proliferation of Artificial Intelligence (AI) has impacted virtually every aspect of modern life, altering the course of human advancement in a countless number of fields ranging from science, technology, healthcare, and transportation, to finance and entertainment. But as the saying goes, with great power comes great responsibility. To that end, the Federal Government has taken a particular interest in one application of AI—national defense.

AI can be used, for example, to ingest multiple terabytes of drone or satellite footage in real-time, connect data points using sophisticated machine learning algorithms, and provide real-time assessments to combat troops and intelligence operatives. Or, it can collect social media feeds and camera footage, apply facial-recognition capabilities, and alert the authorities to suspicious activity, all in real-time and with precision accuracy. These programs, and others like them, are of extraordinary value to U.S. national security interests. And for home-grown technology, the U.S. is developing a regulatory framework to prevent AI (with military capabilities) from falling into the wrong hands. What follows is a brief introduction to this regulatory framework. Specifically, even companies that develop commercial (*i.e.*, non-military) AI—or operate in a supply chain whose vertical incudes AI—may be required to register and comply, and penalties for violations, even if inadvertent, can be severe.

The International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) both govern the export and import of items and technology relevant to national security. Moreover, the Committee on Foreign Investment in the United States (CFIUS) enforces the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which governs foreign investment in companies that export sensitive items or data.

International Traffic in ARMS Regulations (ITAR)

The U.S. Department of State administers the ITAR, which governs "defense articles," "defense services,"

and related "technical data" identified on the ITAR's U.S. Munitions List (USML). In order to begin steps to comply with ITAR, companies must register with the Directorate of Defense Trade Controls (DDTC). Although registration does not confer any export rights or privileges, it provides the U.S. Government with information on who is involved in certain manufacturing and exporting activities, and is generally a prerequisite to the issuance of any license or other approvals. An overview of the registration process can be found on the DDTC website.

Several recent amendments to the ITAR are particularly important to AI companies. Effective March 25, 2020, the Department of State amended certain sections of the ITAR to clarify requirements regarding technical data. Specifically, the Department added §120.54(a)(5):

It is ***not a controlled event to send, take, or store unclassified technical data when it is effectively encrypted using end-to-end encryption***. Therefore, a controlled event does not occur when technical data is encrypted prior to leaving the sender's facilities and remains encrypted until decrypted by the intended authorized recipient, or until retrieved by the sender, as in the case of remote storage. The controlled event occurs upon the release of the technical data. If the technical data is decrypted by someone other than the sender, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, then the technical data is not secured using end-to-end encryption for purposes of paragraph (a)(5) and the original transmission was a controlled event.

Since the ITAR is concerned with 'export' to a 'foreigner,' it is important to understand how the ITAR defines each of those terms. First, the ITAR defines "person" to include corporations and entities. [120.14]. The ITAR then distinguishes between a "U.S. person" and "foreign person" based on permanent residency (*i.e.*, citizenship not required). And for entities, whether it is incorporated in, or does business in, the U.S. [120.15]. A "foreign person" is any person or entity that is not a "U.S. person." [120.16]. Below, are several examples of how these conditions interpreted by ITAR.

- Any release of technical data to a foreign person is a controlled event, even if that foreign person is in the U.S.
- Release of technical data to U.S. persons within the U.S. is not a controlled event.
- Release of technical data between two U.S. persons in the same foreign country is not a controlled event, but a release between those same U.S. persons in different foreign countries is a controlled event.

It is important to remember that, for unclassified and properly encrypted exports of technical data, these conditions are superseded by the recently added terms of 120.54(a)(5).

The ITAR focuses on proper encryption of technical data and on ensuring that only intended recipients have access to exported technical data. However, AI companies subject to the ITAR should consider developing a robust, well-documented compliance program to enhance the likelihood of compliance and serve as a mitigating factor in the event the company is accused of an ITAR violation. A robust compliance program should include at least the following:

- End-to-End Encryption, as described above.
- Access Controls: set expiration, disable forwarding capabilities, revoke access in the event of a breach, and watermark files.
- Persistent Protection: ensure compliance beyond initial transmission and maintain control of attachments.
- Data Loss Prevention: automatically enforce encryption and access controls by detecting ITAR data in emails and attachments.

- Routine Audit: review the dissemination of ITAR data and ensure compliance throughout the entire supply chain.
- Key Management: host your own keys to prevent unauthorized access.

It is important for AI companies to remain current on any developments or rule clarifications regarding the ITAR. They should keep in mind not only their registration and licensure requirements and whether their technology falls under ITAR regulations, but also the identity and residency of end users of the technology, the ITAR prohibited foreign countries, applicable exemptions to "controlled events," and reporting requirements.

If a company is unsure of its obligations with regard to ITAR compliance, it may request an interpretation in the form of an advisory opinion from the DDTC. [126.9(c)].

Export Administration Regulations (EAR)

Administered by the Bureau of Industry and Security (BIS), the EAR controls the export of: (1) "dual use" items, defined as items that have "civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications"; and (2) items exclusively used for military applications but that do not warrant control under the ITAR [730.3]. Although the core of the EAR provisions relate to exports from the United States, some EAR provisions broadly define the term "export." Additionally, some EAR provisions can also apply to transactions outside of the United States, or apply to activities other than exports [730.5].

As a result of the broad definition of the term "export" under some EAR provisions, certain actions that may not constitute an export in other contexts will constitute an export subject to the EAR. For example, the following actions would constitute an export subject to the EAR: (1) the release of technology to a foreign national in the United States through means such as demonstration or oral briefing; (2) the return of foreign equipment to its country of origin after repair in the United States; (3) shipments from a U.S. foreign trade zone; and (4) electronic transmission of non-public data that will be received abroad [730.5(c)].

Activities other than exports that are covered by EAR provisions include the following:

- **Re-exports**: commodities, software, and technology that have been exported from the United States are generally subject to the EAR with respect to re-export. However, many re-exports may go to destinations without a license or will qualify for an exception from licensing requirements [730.5(a)].
- **Foreign Products**: authorization to export technology from the United States may be subject to assurances that items produced abroad as a direct product of that technology will not be exported to certain destinations without authorization from the BIS [730.5(b)].
- **U.S. Person Activities**: to counter the proliferation of weapons of mass destruction, the EAR restricts the involvement of U.S. persons anywhere in the world in exports of foreign-origin items, or in providing services or support that may contribute to such proliferation [730.5(d)].

Although the BIS and other agencies that maintain export-related programs try to minimize overlapping jurisdiction, items and activities subject to EAR controls are not necessarily exempted from other control programs, and compliance with more than one regulatory program may be required [734.2(3)].

Items and activities subject to EAR controls are defined in Part 734, which "provides the rules you need to use to determine whether items and activities are subject to the EAR" [734.1(a)]. The definition of "items subject to the EAR" includes, *but is not limited to*, items listed on the Commerce Control List. [730.8(2), emphasis added].

To date, the EAR has taken a very narrow approach to restricting AI. On January 6, 2020, the Department of Commerce issued restrictions on exports and re-exports of AI software designed to analyze satellite images, specifically to "geospatial imagery 'software' 'specially designed' for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds." However, as AI continues to advance, the EAR will likely broaden these restrictions. AI companies should remain aware of any future developments with regard to the EAR.

Committee on Foreign Investment in the United States (CFIUS)

As AI advances, so too does investor interest. In 2018, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA) which expanded the power of the CFIUS to provide increased oversight of foreign investments in the United States AI market to prevent threats to national security, as well as to prevent U.S. competitors from improperly gaining access to critical technologies.

Items and technology controlled by either the ITAR or EAR will also be considered as critical technology by CFIUS for both voluntary and mandatory CFIUS purposes. Thus, a determination under ITAR or EAR that an AI company's technology is "critical technology" means that certain financial transactions (e.g., transfer in control or foreign investment) may be subject to additional scrutiny by CFIUS.

The intellectual property group at Shumaker continues to advise AI companies on all areas of IP, as well as related topics, such as these export regulations. We also advise non-AI clients on export control related matters, including interpretation and application of the ITAR, EAR, and CFIUS. If you would like to discuss any of these issues, please give us a call.

Please do not hesitate to contact Tom BenGera at tbengera@shumaker.com or 704.945.2193, or Patrick B. Horne at phorne@shumaker.com or 704.945.2902, if you have any questions.