epiq

WHITE PAPER

Mitigate Risk in Handling eDiscovery Data Subject to the U.S. Export Control Laws and Regulations

The corporate world continues to see exponential growth in the generation of electronic data as a bi-product of business activity. Along with this growth come a number of responsibilities associated with the duty to preserve, identify and transfer data, particularly when dealing with electronic discovery. In the context of document review and how data is delivered to an electronic discovery vendor, certain regulations need to be given careful consideration before that information changes hands.

There are several domestic regulations to consider, such as the Health Information Portability Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA), each of which imposes special handling requirements for data. In addition, international regulations such as blocking statutes and data protection laws complicate data transfers across national boundaries. In this paper, however, we focus on one of the less understood regulations that aim to protect the transfer of knowledge relating to military technology.

U.S. Export Control Laws and Regulations

The Export Administration Regulations ("EAR"), enforced by the United States Department of Commerce, and the International Traffic in Arms Regulations ("ITAR"), enforced by the United States Department of State, require that businesses in selected industries take steps to ensure the security of data that could assist in the development of military capability. Together EAR and ITAR are referred to as the "U.S. Export Control Laws and Regulations" ("Regulations"). Any corporation that conducts business in the aerospace, defense, automotive, chemical, engineering, construction and high tech industries is subject to these regulations. This means that these corporations must control their data sufficiently to avoid the "export" of this type of information outside the United States without a license and to prevent access by "foreign persons."[1]

Violations can result in substantial penalties. Individual liability for the disclosure of controlled technical data to unauthorized foreign persons under the ITAR includes fines of up to $500,000 per violation for civil violations and up to ten years of imprisonment along with penalties of up to $1,000,000 per violation for criminal violations. Liabilities under the EAR may involve fines ranging from $10,000 to $120,000 for each civil violation and fines ranging from $50,000 to $1,000,000 for each criminal violation with 10 years of imprisonment.

[1] See 22 C.F.R. § 120.9 (2007).
[2] See id. § 120.16.
[3] See id. § 120.10.
[4] See id. § 120.17.

What is a Foreign Person?

A "foreign person" is anyone who is "not a lawful permanent resident" of the United States (i.e., not a United States citizen or green card holder) or does not have refugee or asylum status.[2]

What is Export Controlled Data?

In general, "export controlled data" includes specific information needed to develop, produce, maintain, manufacture, assemble, test, repair, operate, modify, process or otherwise use equipment or technologies that are on the control lists of the EAR or the ITAR. Export controlled data may take the form of "blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories."[3]

"Corporations must control their data sufficiently to avoid the "export" of this type of information outside the United States without a license and to prevent access by 'foreign persons.'"

Implications for Service Providers

It is therefore critical for any business that possesses data subject to the U.S. Export Control Laws and Regulations to maintain strict protocols for any and all transfers of technical data, as the definition of "export" is quite broad under the Regulations.[4] This responsibility extends to any third party providing services to the owner of the data, including outside counsel and any electronic discovery company, so particular caution must be used when utilizing legal services such as data collection, litigation support or database hosting.

Once an electronic discovery company has been contacted by a corporation or its outside counsel to provide legal services, certain key questions need to be asked to assess whether steps should be taken to ensure compliance with the Regulations. These questions include whether the client conducts business within the affected categories under the ITAR or EAR, and whether technical data may be included in the submitted data set.

Prohibited Activities

Data subject to the Regulations must not be, inter alia, exported, provided or made accessible to foreign persons. This includes the following activities: sending a copy, providing access to the data, sharing it or disclosing it in any form, including written, verbal and visual.

Avoiding Inadvertent “Export”

Data “export” is interpreted broadly, so it is critical to ensure that the data is appropriately secured with access provided only to authorized users who are not foreign persons. Accordingly, any employee assigned to the project should be required to sign a certificate stating that s/he:

- is familiar with the export control issues involved in the matter and understands the certification.
- is aware of his or her personal liability upon a disclosure of export controlled technical data to foreign persons.
- agrees to take reasonable measures to prevent unauthorized foreign persons from having access to or using any export controlled technical data.
- is required to contact a supervisor in connection with any type of disclosure of export controlled technical data including without limitation to any foreign person

Additional Recommendations

Identify the Data

Ensure that protected data is always clearly identifiable by implementing the following measures:

- Require that the client clearly mark and identify any export controlled technical data.
- Secure physical data in a separate, access restricted, enclosed, locked room.
- Clearly label the room as a secure, access restricted space.

Isolate the Data

Additionally, implement the following measures to keep the data from being inadvertently viewed by a foreign person:

- Create a secure, separate database to hold the data.
- Take all commercially reasonable measures to secure the data.
- Implement a separate user account creation process that requires the human resources department to verify the non-foreign person status.
- Disable or monitor any remote access to the data

Identify Customer Service Group

Clients who own export controlled data will need to communicate with the client services team regarding deliveries, data processing and other document review-related issues during the litigation. Customer service team members must not be “foreign persons;” therefore, identify U.S. nationals to serve as dedicated client service representatives.

Coummunicate Internally

Electronic discovery service providers that deal with data subject to the U.S. Export Control Laws and Regulations should prepare and distribute memoranda and checklists to the entire company describing requirements regarding the data set, and regularly train and educate employees. As an example, the following is a list of recommended actions:

- Hire outside counsel to assist in developing compliance protocols.
- Designate a permitted list of vendor employees who are authorized to access the data.
- Make sure that each employee has passed a criminal background check.
- Require that any employee being given access to such data executes a document certifying his/her willingness to comply with the Regulatory requirements before being granted access to the data. Have each employee sign a copy and return it to the HR Administrator or legal department.
- Have the client or its outside counsel provide a list of client employees who can have access to the data. If the client wants to give additional employees access to the data, require the client or its outside counsel to update this list regularly and accordingly.
- Require that work on the project be done within a secured space with self-locking doors and with authorized access only.
- Disable any feature on workstations that can allow users to download information, such as USB ports, CD writers and floppy disk drives.
- Allow hardcopy printing to be performed only in access controlled spaces and require employees to shred printed documents.
- Escalate all questions to a supervisor, corporate legal department or outside counsel.

The risks of handling data subject to U.S. Export Control Laws and Regulations are substantial. However, by designing an appropriate infrastructure and implementing some of the protocols recommended herein, these risks can be mitigated. Such protocols require an investment of time, personnel and financial resources to ensure compliance.