
Ask the Expert - Mark D. Menefee, Baker & McKenzie LLP

QUESTION

"Foreign National licensing – "The "Foreign National" is employed in a Canadian subsidiary. His work involves IT which means his U.S. counterparts want to provide him access to specific networks, servers and programs to enable him to fulfill his IT responsibilities.

His main project is a configuration management tool for a "requirements database". According to his counterpart in the US, he does not necessarily look at the data, but he manipulates the program that provides the data to research administrators. However, he would be able to access the data. It is important to note that each network, server and application requires a login/password to restrict and limit access."

A precise analysis of the export compliance issues arising from this scenario would be very fact dependent. Nevertheless, we can sketch out some basic steps you should follow in determining how the U.S. export laws might apply to your situation.

There are basically two export compliance questions to consider when analyzing a problem like this: (1) what are the export control classifications of the information in the company's network? and (2) would that information be released or transferred to this IT employee? Based on your answers to those questions, you might also need to consider some employment law issues.

Let's start with the classification issue first. The question doesn't provide specific information about what information is in the company's network. However, since there is a reference to "research", let's make the most cautious assumptions possible.

The information flowing through a company's network could be of three types: (1) not subject to U.S. export controls (e.g., information that is already publicly available, such as sales brochures posted on the internet and freely available for downloading); (2) subject to the Export Administration Regulations ("EAR") (e.g., software specifically designed to operate a 5 axis machine tool, or proprietary design drawings for a circuit board); or (3) subject to the International Traffic in Arms Regulations ("ITAR") (e.g., technical data concerning the avionics package for a F-15 fighter plane). To save space here, we'll leave aside the question about how Canadian export control law would apply, but you should examine that carefully also.

Depending on how the information in the network is classified, an export license might be required for that information to be released or transferred to a foreign national working in Canada. Under the EAR, this might be considered to be a "deemed reexport."

Before we talk about a deemed reexport, let's discuss what is a "deemed export." Subsection 734.2(b) of the EAR sets forth the deemed export rule, as it is called. This subsection provides that the export of technology or software includes "any release of technology or source code subject to the EAR to a foreign national." Such a release is "deemed to be an export to the home country or countries of the foreign national." In other words, even though a foreign national might be located physically within the U.S., release of technology or source code to him or her is deemed to be an export, as if the person took the item back to his or her home country. Likewise, a release of technology or source code subject to the EAR to a foreign national, when it occurs outside of the U.S., is considered to be a deemed reexport. For example, if an Indian national is working temporarily in your company's Canadian subsidiary, the release of technology subject to the EAR to him or her would be a deemed reexport to India. Licensing policy regarding India, not Canada, would apply.

The deemed export and reexport rules do not apply to everyone, however. For releases of technology and software in the U.S., no deemed export occurs if the recipient is: (a) a U.S. citizen; (b) a foreign national who has become a lawful permanent resident of the U.S.; or (c) a foreign national who has been formally granted political asylum or political refugee status in the U.S. In other words, the deemed export rule applies only to foreign nationals who are temporarily in the U.S., such as people traveling to the U.S. under a student or business visa.

It gets more complicated for a foreign national who is working outside of the U.S. According to Subsection 734.2(b)(5), the same exclusion applies for persons who are lawfully admitted for permanent residence in the foreign country. We could use some clarification from the U.S. Commerce Department concerning what constitutes lawful permanent residence under non-U.S. laws, including those of Canada, for the purposes of the deemed reexport rule.

How does a "release" of technology or software occur? The EAR says it can occur by (a) visual inspection; (b) oral exchanges of information; or (c) the application to situations abroad of personal knowledge or technical experience acquired in the U.S.

What is "technology"? The EAR define it as specific information necessary for the "development," "production," or "use" of a product.

The ITAR do not expressly use the concept of "deemed export" but they reach a similar result. ITAR Section 120.17 defines an export to include "Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." Also included in that definition is "Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad."

Under the ITAR, technology contained in email traffic or stored in a company's intranet database which could be accessed by the network administrator would be considered by the regulatory authorities to be transferred or disclosed to that administrator.

The leading enforcement case on this point is In the Matter of General Motors Corp. and General Dynamics Corp., which was settled on November 1, 2004, with the imposition of a \$10 million civil fine on each company. That case involved a Canadian subsidiary of General Motors which manufactured the Light Armored Vehicle for the U.S. Army. General Dynamics acquired the subsidiary after the violations occurred.

The manufacturing was performed under a Technical Assistance Agreement issued by the U.S. State Department's Directorate of Defense Trade Controls ("DDTC"), which prohibited unauthorized foreign nationals from having access to the technical data. DDTC took the position that by failing to restrict access to the intranet data by employees who were "dual nationals" (that is, they were citizens of Canada and another country, e.g., China), the company had transferred or disclosed technical data to them illegally. The settlement documents for that case can be found on DDTC's website (<http://www.pmdtc.org/>).

According to DDTC's interpretation, the transfer or disclosure of technical data did not actually have to occur for there to be a violation of the ITAR. Merely failing to restrict access was sufficient.

On its website (www.bis.doc.gov), BIS provides some FAQ's concerning deemed exports and deemed reexports. There BIS states that "Technology is 'released' for export when it is available to foreign nationals for visual inspection...." Thus, it is likely that would similarly conclude that technology would be released to the IT person by virtue of mere access.

To complicate matters further, suppose the network does contain some technical data that is subject to control under the ITAR or the EAR and would require a license for the IT person. This situation could raise employment law and data privacy issues under Canadian law for the company. While U.S. employment law (Title VII of the Civil Rights Act) generally prohibits discrimination based on national origin, it does provide a narrow exception for national security. But it is possible that Canadian employment law does not do so. Even if Canadian law does provide a comparable exception, the exception might not contemplate the national security concerns of another country. Moreover, Canada's data privacy law is quite strict and may prevent your company from asking about the IT person's nationality. Therefore, if you think your company might be facing a possible conflict between U.S. export control laws and Canadian employment and/or data privacy laws, you should consult your attorneys in both countries.

Thus, the "release" part of the question is relatively easy to answer, even though you might not agree with the interpretations of DDTC or BIS. The classification part of the question can be challenging. Proper management of the employment and data privacy issues relating to a job that requires licensed access to technical information can require the export compliance administrator and the human resources manager to work closely together to ensure that the company remains in compliance with all laws.