Export Controls Alert

Recent developments in export controls

A publication of Nixon Peabody LLP

AUGUST 4, 2011

The export control implications of cloud computing

By Alexandra López-Casero

When do cloud users and providers become "exporters" under U.S. export controls? Did you know that uploading technical data to the "cloud" can expose you and your organization to violations of U.S. export laws? For example who is the exporter if a U.S. company places its technical data with a U.S. provider, but the data is actually transmitted via a router in Germany for ultimate storage in India? The wrong answer can result in both civil and criminal penalties under the export laws. This alert discusses how cloud computing implicates U.S. export control laws and how the U.S. Government has and might respond to violations. It also provides recommendations on export compliance "in the cloud" for cloud users and providers.

Cloud computing is transforming how IT and software applications are used. The recent outages of Microsoft's BPOS cloud-hosted communication and collaboration suite and the well-publicized Amazon cloud outage last spring have highlighted important questions about the reliability of cloud computing. Despite these glitches, most analysts agree that cloud computing will be a driving force in corporate information management because it is cheaper and more efficient than using corporate resources. According to Gartner Inc., the global market for cloud-related services may surge from $68 billion in 2010 to almost $150 billion in 2014. Last week, the U.S. General Services Administration announced that it migrated all of its employees to a cloud-based e-mail service using Google Apps for Government, as part of the Obama administration's plans to move a portion of its IT capabilities to the cloud within 18 months.

The most obvious concerns about cloud computing are security and privacy. However, cloud providers and, particularly, cloud users must pay close attention to how U.S. export control laws affect cloud computing. Last week, the Brookings Institution, a Washington-based think tank, dedicated a report on the export controls challenges posed by cloud computing. The implications of export controls for cloud computing are not obvious and the U.S. Government has provided limited

guidance. However, the reach of U.S. export controls is broad, and violations of U.S. export controls can trigger substantial civil and criminal penalties, including loss of export privileges.

Inherent tension between trans-national character of cloud computing and export controls

Some of the key features and functional benefits of the cloud are scalability, virtualized resources, and portability. A cloud's routers, servers, and technical data storage devices are typically positioned across multiple systems—oftentimes across the globe. A U.S. company that uploads technical data to the cloud of a U.S. provider typically does not know where its data will be stored within the cloud. It may be routed through the Netherlands and stored on a server in Singapore or elsewhere. U.S. export control laws, however, are designed to regulate the shipment and transmission of controlled products, software, and technology across national borders. Thus, knowing the actual trajectory and physical destination of technical data is essential to understanding whether a transmission of technical data requires an export license from the U.S. Government and the degree of compliance that is required. Cloud computing, therefore, poses unique export compliance challenges for cloud users and providers, in addition to the compliance issues that already exist in any other Internet context.

How has the U.S. Government responded?

Of the three federal government agencies that administer U.S. export laws, only the Bureau of Industry and Security ("BIS") at the Department of Commerce has formally addressed the export controls implications of cloud computing.

Two advisory opinions from the Department of Commerce

BIS, which administers the Export Administration Regulations ("EAR") for so-called "dual-use" products,[1] has issued two advisory opinions on cloud computing. Both advisory opinions provide helpful insight on BIS's perspective on some of the legal issues posed by cloud technology. However, they only address a limited range of scenarios and, more importantly, put the burden of compliance on the user (not the provider) of cloud computing services.

2009 Advisory Opinion: provision of cloud computing services alone is not an "export"

In January 2009, BIS issued its first advisory opinion on cloud computing (the "2009 AO"), which had been requested by an unnamed provider of cloud computing services. In this AO, BIS concluded, among other things, that:

---

[1] "Dual-use" items are items that have both commercial and military or proliferation applications, such as most computers, software, machine tools, and telecommunications equipment. While the term "dual-use" is used informally to describe items that are subject to the EAR, purely commercial items are subject to the same regulations.

- *Providing computational capacity* (a service) is not by itself an "export" and, therefore, not subject to the EAR;
- *Shipping or transmitting software* that is subject to the EAR to a foreign destination (or a foreign person in the U.S.) to enable cloud computing is an "export" and subject to the EAR;
- *Shipping or transmitting technology* that is subject to the EAR to a foreign destination (or a foreign person in the U.S.) in the form of technical data (for example, manuals or instructions) or technical services to show a user how to access and use the computational capacity of a cloud is an export and subject to the EAR;
- *Exporting controlled software or technology to and from the cloud* is subject to the EAR;
- *The cloud provider in the U.S. is* generally not the exporter of any data that users place on and retrieve from the cloud because the cloud provider does not receive the "primary benefit … of the transaction"; and
- *The cloud user abroad* is generally not the exporter because it is not located in the U.S.

Let's look at the following scenario to illustrate these findings. Assume a user based in the U.S. places technical data, which would require a license to export it from the U.S., on a provider's U.S.-based cloud, and the data is downloaded by a third party in India. Who is the exporter? Based on the 2009 AO, the *cloud provider* is not the exporter because providing computational capacity by itself (a service) is not an export and because the provider is not receiving the "primary benefit of the transaction." The third party in India is not the exporter because it is not located in the U.S. The U.S. company that uploaded its technical data onto the provider's cloud did not directly export the data, but it is receiving the primary benefit of the cloud services and, therefore, is ultimately responsible for ensuring that no foreign person has access to its technical data. In an enforcement action, the government would likely hold the U.S.-based user accountable for the unauthorized export to the third party in India.

By concluding that *providers* of cloud services are generally not the "exporters" of controlled technical data that users place on and retrieve from the cloud, the 2009 AO put the responsibility of export compliance largely on the cloud *user*. However, the 2009 AO only addresses a limited cloud computing scenario. Each fact pattern must be considered on its own merits. Moreover, BIS does not speak for the other federal agencies that administer U.S. export laws.

2011 Advisory Opinion: cloud providers that employ foreign IT staff are not "deemed exporters"

In a second advisory opinion in January 2011 (the "2011 AO"), BIS confronted the related question as to whether cloud providers need to obtain "deemed export" licenses for their foreign national IT administrators who have access to users' controlled technology. BIS concluded that because a cloud provider is generally not the "exporter," it is not "deemed" to be an exporter. As others in the export controls community have pointed out, this conclusion seems at odds with the concept of a "deemed

export."[2] Moreover, the 2011 AO seems to put the onus of a potential deemed export again on the cloud user. If the cloud provider and the foreign IT administrator are not exporters, deemed or otherwise, the user is the only remaining "exporting" party. Thus, in theory, the user should ensure that its technology is not accessible by foreign persons (such as the provider's foreign IT administrators). Therefore, cloud users should have safeguards in their cloud computing arrangements to bar cloud providers from allowing their foreign network administrators to monitor user-generated technology controlled by U.S. export laws.

No formal guidance from the U.S. State and Treasury Departments

The State Department's Directorate of Defense Trade Controls (the "DDTC"), which administers the International Traffic in Arms Regulations ("ITAR"), has not provided any formal guidance on the implications of cloud computing. The "export" definition under the ITAR is broader than under the EAR, and based on informal discussions with the DDTC, the DDTC will likely scrutinize even mere uploads of ITAR-controlled technical data to the cloud (let alone actual transfers or downloads). An export under ITAR includes visually disclosing or transferring technical data to a foreign person, whether in the United States or abroad. The DDTC will likely take a strict position as to whether cloud users of ITAR-controlled technology and software have ensured that adequate measures are in place to prevent unauthorized foreign nationals from having access to controlled technology or software, regardless of where it is located. Some cloud providers offer "ITAR-compliant" clouds. While geographic restrictions are certainly useful, providers and users of "ITAR-compliant" clouds should be aware that they will likely put themselves under increased scrutiny. It seems likely that the DDTC would want corroboration that the applicable cloud is indeed ITAR-compliant.

The Treasury Department's Office of Foreign Assets Controls ("OFAC"), which administers and enforces economic and trade sanctions, has also not expressed a formal position on cloud computing. However, OFAC will likely take issue with the provision of cloud computing services to blocked persons or embargoed countries, regardless of whether or not BIS views a cloud provider as an exporter.

What can cloud users and providers do to step up their export control compliance?

Cloud computing creates an increased likelihood of unintentional export control violations, particularly by cloud users. Below are examples of basic compliance measures that cloud users and providers should consider to assess their existing compliance, explore a suitable compliance program, and take any corrective actions.

---

[2] In the typical export scenario, data is transmitted across national borders. In a "deemed export" scenario, a person who makes controlled technology available to a foreign national in the U.S. is "deemed" to be an exporter, even though the data is not transmitted across national borders.

Recommendations for cloud users

Cloud users should start with the same compliance measures they use for "traditional" exports and re-exports of controlled software and technology. They should have a good command of the regulatory regimes, export control classifications, and licensing requirements applicable to their technology and software in the cloud. Their export compliance officers need to clearly understand what is going to happen to their data once it is in the cloud, i.e., what data will be uploaded, transferred, or downloaded from the cloud, and when and by whom. Cloud users should incorporate cloud computing into their company-wide export controls policies and, for example, implement restrictions on employee transfers of controlled technical data and software to and from the cloud. Users should also carefully review their agreements with cloud providers and consider how and where their data will be stored and how they may be affected by limitations on liability. Moreover, cloud users should consider agreeing with cloud providers on a designated geographic area (the U.S. or a designated list of countries, depending on the applicable export control restrictions) where the user's controlled technology or software may be stored. This can be difficult as many cloud providers may not be able or willing to tell users where their clouds are located or on which clouds user data is stored. In that case, users may want to decide to use clouds with already defined locations rather than cloud providers who are more secretive about the locations of their clouds. In addition, cloud users should consider limiting cloud computing to items that are not subject to the EAR or classified at the EAR99 (no license required) level. Users will also want to ensure (and incorporate adequate provisions into their cloud computing arrangements) that cloud providers put appropriate measures in place to prevent unauthorized foreign nationals from accessing controlled technology and software wherever located. However, users should be aware that no contractual arrangement with a cloud provider, however carefully drafted, will shift the onus of export compliance to the cloud provider. Regardless of any legal remedies that a user may have against a cloud provider that violated its contractual compliance obligation to implement adequate safeguards against unauthorized access by foreign nationals, from a government enforcement perspective, the user would still be on the hook and responsible for export controls violations concerning its controlled technical data or software. Finally, cloud users who want to use cloud computational services for their EAR-controlled technology or software may want to consider obtaining a license from BIS for multiple exports or reexports to and from the cloud.

Recommendations for cloud providers

Cloud providers need to explore and analyze those scenarios when they may cross the line and no longer only provide computational services but actually "export" technology or software that is subject to the EAR and does not derive from a cloud user (such as proprietary, non-publicly available software instructing a cloud user how to access and use the cloud). Cloud providers should also assess whether trouble-shooting requires the transmission of controlled technical data. Moreover, cloud providers should strengthen their IT security over cloud infrastructure to prevent unauthorized access to data uploaded by users to the cloud.

In addition, cloud providers should consider offering users some level of control over the physical location of cloud resources and the option to restrict their computations to servers in the United States.

Conclusion

Cloud computing presents unique export controls challenges. The different federal regulatory agencies controlling exports have only provided limited guidance. It is clear that every time controlled technical data is uploaded, transferred, or downloaded from and to an international server, it is "exported" and may thus be subject to the U.S. export control laws. What is not clear is how the respective agencies will view these "exports" under applicable export laws. Cloud users and providers should examine their internal compliance procedures and safeguards and identify areas that need improvement. Cloud computing should be incorporated into the internal compliance program of cloud users and providers alike. Companies should start with the same compliance measures they use for traditional exports and re-exports of controlled software and technology and adapt these concepts to cloud computing. What specific export controls compliance measures are necessary must be addressed on a case-by-case basis and requires a good command of the regulatory regime(s), export control classifications, and licensing requirements applicable to specific technology and software. Getting the necessary internal support to implement and maintain an effective export compliance system can be challenging. However, companies that neglect to comply risk heavy fines and potential loss of export privileges and company reputation in the event of an enforcement action.

For more information, please contact:

- Alexandra Lopez-Casero at (202) 585-8372 or alopezcasero@nixonpeabody.com
- Peter Durant at (585) 263-1227 or pdurant@nixonpeabody.com