Law360
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

US Export Controls And Cloud Computing

Law360, New York (September 10, 2010) -- Many companies are only beginning to grapple with the U.S. export control implications of "cloud computing," a method of using the Internet to access third-party information technology resources for using and developing software applications and for obtaining storage, processing and bandwidth resources.

Cloud computing providers ("providers") offer various services, including webmail, back-up storage capacity, and tools for software development, and may offer a broad array of such services or specialized services in areas such as customer relationship management or financial transactions, among others.

Cloud computing users ("users") can be individual consumers, businesses of any size, or government agencies, and these users typically opt for cloud computing to outsource selected IT functions (and thereby reduce the need for larger IT staffs or IT infrastructure), facilitate ease of data access, and/or collaborate on software and technology projects.

Cloud computing, like any activity using remote computing access, might involve technology and software exports, but three aspects of cloud computing present unique challenges to companies.

First, cloud computing involves "virtualized" resources (e.g., servers) where the user might not be aware of exactly which provider server it is accessing or where the server is located. Moreover, user data stored "in the cloud" might be on one server during one session and on another server during the next.

Second, because users access cloud computing services via the Internet, the provider might not know in advance where the user will be located at the time it accesses the cloud.

Third, with "traditional" software or technology transfers, a company or a third-party acting on behalf of the company (e.g., a freight forwarder) exports from the country in which it is located (e.g., the company exports software from its office in the United States to South Korea), but with cloud computing, the software or technology often is exported from the location of the provider, not the user. Thus, a cloud user in the United States might transfer software from a provider's server in Canada to a colleague in China.

This article highlights certain issues that arise in the context of cloud computing involving exports of software or technology subject to the Export Administration Regulations ("EAR") (collectively, "controlled data"). The EAR govern exports of commercial/dual-use items and are administered by the U.S. Commerce Department's Bureau of Industry and Security ("BIS"), which has addressed some of the implications of cloud computing. The article concludes with suggested compliance measures and a note on the future of U.S. trade controls governing cloud computing.

Cloud Computing Implications Under the EAR

As noted above, one of the most challenging aspects of export compliance in this area involves determining the locations of the controlled data and the user. Nonetheless, given the focus of the EAR on the country of export and the country of destination, a useful framework for analyzing the implications of export controls on cloud computing is to examine the locations of the cloud computing resources and the user.

Provider Resources Abroad/User in the United States

The most straightforward analysis of the U.S. export control implications of cloud computing involves a user in the United States and cloud provider resources abroad. Such transactions are similar to other electronic exports of technology or software (e.g., via e-mail). Under the EAR, if the user transmits controlled data to the cloud — for example, by saving a file to a cloud server abroad — an export has occurred. The user must ensure that such exports comply with the EAR.

Provider Resources in the United States/User Abroad

In a January 2009 advisory opinion, BIS addressed the scenario in which the provider's resources are in the United States and the user is abroad. Addressing the scenario from the provider's perspective, BIS clarified that merely providing a cloud service is not an activity subject to the EAR. If, however, the provider transmits controlled data to the user abroad, an export has occurred.

BIS concluded that if the user exports controlled data stored on the provider's servers in the United States, the provider generally would not be the exporter because the provider would not be receiving the "primary benefit ... of the transaction."

BIS also concluded, however, that the user could not be the exporter because the user is not in the United States. BIS's conclusions are consistent with the language of the EAR, but they leave the identity of the exporter unclear in this type of export transaction.

All parties to export transactions must comply with the EAR, but by leaving open the question of who the exporter is under this scenario, BIS appears to acknowledge that the EAR does not yet effectively address how to analyze situations in which a user abroad initiates an export from a provider's server in the United States.

BIS clarified that the provider in the United States generally would not be responsible for exports initiated by users abroad, but the advisory opinion — because it addressed a requester's specific set of questions — left a number of issues open to interpretation:

- What are the full extent of the user's obligation to comply with the EAR under the scenario above, given that the user in real-time typically will know or should know the destination of the controlled data downloaded or transferred from the provider's servers in the United States?

If a user in the United Kingdom, for example, transfers U.S.-origin software from the provider's server in the United States to China, would the user not have some obligation to comply with the EAR, even if the user is not the "exporter" (because it is located outside the United States)?

Such a transfer closely resembles a reexport of U.S.-origin software, and it would appear that if the user does not have some obligation to comply with the EAR, an absurd result would obtain — a user abroad could avoid the EAR's licensing requirements by storing the software on a provider's server in the United States. But, again, the precise contours of the user's obligations under the EAR are unclear.

- If the cloud provider is not generally transparent about the locations of its servers and the user does not know in which country its controlled data are stored, what are the user's obligations to comply with the EAR?

- Would foreign-origin software or technology of a user abroad be subject to the EAR it were stored on a provider's server in the United States? Generally, commercial software or technology located in the United States is subject to the EAR (regardless of origin), but would BIS consider a German company's downloading of its proprietary software from a provider's server in the United States an export under the EAR? What if the software initially

was stored on the provider's server in Germany, but the day before the download, the provider — due to a catastrophic IT event — moved the software to a server in the United States?

Provider Resources and User Outside the United States

If the provider resources and user are both outside the United States, compliance with the EAR turns largely, although not exclusively, on whether controlled data that are re-exported — exported from one foreign country to another — are of U.S. origin.

Certain re-exports would be treated like "traditional" reexports involving U.S.-origin software or technology, particularly if the reexporter knows the destination country, but other re-exports to or from the cloud raise the same thorny questions addressed above relating to the exporter's identity and the user's and provider's obligations.

BIS's advisory opinion, however, at least suggests that a cloud provider in a re-export transaction generally would not be responsible for user-initiated reexports of U.S.-origin controlled data from the cloud.

Provider Resources and User in the United States or Within a Single Foreign Country

An easily overlooked aspect of export compliance in the context of cloud computing is the scenario in which the provider and user both are located in the United States.

Under this scenario, providers and users of cloud computing resources should follow standard physical, procedural and electronic measures for controlling deemed exports — the release within the United States of EAR-controlled source code or technology to foreign persons.

For provider resources and users located in the same foreign country, providers and users should adopt similar measures to prevent unauthorized releases of U.S.-origin source code or technology within that country to foreign persons.

Provider Resources and Users in Multiple Countries

Perhaps the most complicated cloud computing scenario under the EAR involves a company with employees worldwide accessing a cloud provider's servers that are dispersed worldwide.

For example, a multinational company with subsidiaries in the United States, France and Japan might select a cloud provider with servers in North America, Europe and Asia (e.g., to reduce communications latency). Another provider might not be transparent about its server locations and might transfer users' controlled data from servers in Dubai to servers in Asia for remote backup storage. Under these scenarios, companies might simultaneously have to cope with the export, re-export and deemed export issues raised above.

Sample Compliance Measures

Despite the unsettled nature of U.S. export controls as applied to particular aspects of cloud computing, providers and users of cloud computing should implement certain export compliance measures for two reasons.

First, some of these measures address "traditional" exports and reexports of controlled data in which providers' and users' obligations under the EAR are clear. Second, for aspects of cloud computing where the export control implications are unclear, these measures provide a means for companies to manage risk. These measures might include determining:

1) Whether the user will download controlled data to access or use resources within the cloud;

2) Where the user's controlled data will be stored;

3) Whether the provider's services will include active involvement in exports or reexports of controlled data;

4) Whether the provider implements measures to deny access by foreign persons to the user's controlled data (or to deny access to any party other than the user);

5) Whether the user will export controlled data to third parties;

6) The regulatory regime, export control classification, and licensing requirements applicable to the controlled data in the cloud; and

7) The end-users, end-uses and country destinations associated with exports of controlled data in the cloud.

Cloud users should address all of these issues at the outset. Moreover, depending on the sensitivity of the controlled data in the cloud or the country in which the service provider is headquartered, users also might consider:

a) not employing cloud computing for certain matters or applications,

b) limiting controlled data in the cloud to that not subject to the EAR (e.g., publicly available software),

c) using providers that restrict server locations to the United States and deny access to foreign persons,

d) agreeing with cloud providers on the countries where the user's controlled data may be stored, or

e) obtaining a license from BIS for multiple exports or reexports to or from the cloud.

Cloud providers should consider including a provision in their standard service agreements indicating that the user must comply with all applicable U.S. and non-U.S. trade control laws and regulations. Moreover, under certain scenarios, providers still might have their own obligations to comply with U.S. export controls.

Finally, providers might implement server-location restrictions or transparent-server practices across their enterprise or consider offering these restrictions as “upgrades” for users.

Outlook

U.S. trade control regulations have not been amended to reflect certain technological advances, including those surrounding cloud computing. As noted above, questions remain regarding the application of the EAR to cloud computing, and these questions apply equally to other regulatory regimes, such as the International Traffic in Arms Regulations and U.S. economic sanctions regulations. At the same time, the Obama administration is considering significant reforms to these regulations.

Ultimately, cloud providers and users would benefit from greater clarity regarding how to comply with U.S. trade control laws under various cloud computing scenarios. For example, BIS and its counterpart agencies might consider certain default rules for situations in which the user is not generally aware of the precise location of its controlled data in the cloud. In the meantime, though, cloud users and providers must do their best to apply traditional rules regarding software and technology transfers to the world of cloud computing.

--By Brian P. Curran, Hogan Lovells LLP

Brian Curran (brian.curran@hoganlovells.com) is an associate with Hogan Lovells in the firm's Washington, D.C., office and a former analyst with the Defense Intelligence Agency.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360.
