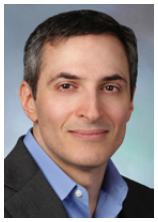
Daily Journal

October 22, 2014

Navigating the cloud: key regulatory issues to know

Behnam Dayanim *is partner and global co-chair of the privacy and data security practice at Paul Hastings LLP.*



Paul Schwartz *is special advisor to Paul Hastings LLP and Jefferson E. Peyser Professor at UC Berkeley School of Law, where he is also a director of the Berkeley Center for Law and Technology.*

While use of the cloud is increasingly attractive to multinational business, significant regulatory implications are associated with its use. Two areas of regulation are the most significant: data protection requirements and restrictions on the export of technical data and technology. Understanding the issues each presents is essential to structuring a compliant cloud solution.

Data Protection

Most of the rest of the world regulates data privacy with a different approach than the United States. The dominant global model refers to "data protection" and follows the European Union's approach to regulation of the use of personal information. This divergence has profound implications for the cloud.

U.S. regulation of the cloud

U.S. information privacy law does not give government officials the power to block international transfers of information. It rarely requires that a law regulate information processing before it takes place. Personal information processing is freely permitted unless a law specifically forbids the activity or otherwise sets parameters on it. There is an increasingly dense patchwork of laws and regulation about privacy in the U.S.

This regulation includes state information privacy law, which is now of increasing importance. Gridlock at the federal lawmaking level in Washington, D.C. has meant that more regulatory initiatives for privacy occur in the states rather than in Congress. These laws include requirements in some states of "reasonable security" and for safe disposal of personal data. Data breach notification laws now exist in 47 states.

Applying these laws to the cloud is extensive: They typically require that any company follow their strictures if it processes or uses the personal data of a resident of their state. The location of the entity that processes the information is irrelevant.

EU regulation of the cloud

In the EU model, an international transfer of data can only take place to countries that the European Commission has determined provide "adequate" data protection, unless one of several enumerated exceptions apply.

These requirements have led to a host of regulatory complexities, which are only heightened by jurisdictional complexities. The EU's 1995 Data Protection Directive includes arcane rules that apply EU privacy law to a "controller" who "is not established on Community territory," but who "for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State." In the cloud, this provision raises difficult questions about who is a controller

and when there is a use of equipment within the territory of the EU.

The proposed 2012 Data Protection Regulation (not yet adopted) takes a new approach with two alternate tests to jurisdiction. These turn on whether a data controller not established in the EU is engaged in an "offering of goods or services" in the EU, or is "monitoring" the behavior of EU "data subjects." These tests will raise new complex legal issues for cloud providers to navigate.

Controls on Export and Transfer of Technology

Apart from personal data, another area of particular sensitivity implicated by use of the cloud is national export control. The U.S. and many other countries impose controls on the export and disclosure of technology, including technical data and software source code. The transfer of that information to a cloud server located outside of its country of origin in many countries would qualify as an "export," and the ability of a service provider to access that information in some countries would be a "disclosure."

Adding further complexity are U.S. "deemed export" rules. Under those rules, disclosing technology to a non-U.S. national constitutes an export, and a license or other approval is generally required if one would be needed for an export to that national's home country. That rule applies regardless of where the national is located (even if she is present in the U.S.).

Before engaging a cloud provider, a company must consider three questions.

What type of information will be stored there?

Much information requires no license to almost any destination or nationality. The nature of that technology will dictate the levels of control required. A company in a non-sensitive area may find few limitations on its ability to utilize the cloud. Conversely, a company in the most sensitive of areas - such as defense or aerospace - may find its cloud options severely restricted.

Importantly, even a company in a "non-sensitive" industry may possess technology that is sensitive. An analysis of what is in its possession is needed. Even if the company has undertaken this analysis with respect to its products for general export compliance, a cloud assessment necessarily must be broader in its focus, to include even internal technology not provided to customers, if that technology will be hosted on cloud servers.

Where are the provider and its servers located?

Export licensing requirements vary by destination. An export license may be required to some countries but not others. Unfortunately, determining location is not always a straightforward question. The nature of cloud services is such that, often, a provider might locate servers in several jurisdictions. The potential cloud client must assess all unless it decides contractually to preclude storage in certain jurisdictions.

Who will have access to the stored information?

Access is often equated to disclosure under U.S. and other export control laws, and disclosure to a national of a country can be equated to disclosure to that country. Hence, if a license is required for disclosure to Country X, it will be required for disclosure to an employee who is a national of Country X.

Here is where it gets tricky: Limiting an employee's duties based on nationality may run afoul of a country's laws prohibiting employment discrimination - even asking about nationalities could trigger liability. Navigating the divide between permissible and impermissible approaches can present challenges for both the cloud provider and its clients.

Identities of provider employees also are relevant, as disclosure of controlled information to certain persons is prohibited under U.S. (and other countries') sanctions laws. Often, screening these personnel to ensure no "prohibited person" is assigned to a project is delegated to the cloud provider as a matter of contract between the parties.

Is This Hopelessly Complex? A move to the cloud has additional legal complication and, sometimes, unavoidable legal risk. As with other decisions, those exposures must be balanced against the many advantages that cloud services provide. Until national laws catch up to how the provision of technical services has evolved, companies will continue to grapple with varying degrees of success.

Behnam Dayanim *is partner and global co-chair of the privacy and data*

security practice at Paul Hastings LLP.

Paul Schwartz *is special advisor to Paul Hastings LLP and Jefferson E. Peyser Professor at UC Berkeley School of Law, where he is also a director of the Berkeley Center for Law and Technology.*

Previous **Next**

HOME : MOBILE SITE : CLASSIFIEDS : EXPERTS/SERVICES : MCLE : DIRECTORIES : SEARCH : PRIVACY : LOGOUT