Skadden

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

April 3, 2012

Cloud Computing: Understanding Security and Jurisdictional Issues

Few topics in the recent history of information technology have garnered as much attention as cloud computing. To some, it is a revolutionary — and far less expensive — approach to the provisioning and use of computer services. To others, the concept — storing a company's data on servers operated by a third party or using remote applications hosted on a third-party platform — is not new, and there are many who assert that this is merely marketing phenomena. However, there are some important differences with the current proliferation of cloud computing.

First, there is an increasing number of applications available for remote access on an as-needed basis, including applications that companies traditionally purchased and stored on their own computers. Second, there has been a significant proliferation of companies offering remote storage services, including many that cater to small-to-mid-size companies. Finally, and perhaps most importantly from a legal perspective, cloud computing has become a globally provided resource. As a result, a U.S. company that retains a cloud provider might find that its data is stored on computers located in multiple countries, and that such data is constantly "on the move."

'Private' Versus 'Public' Clouds

As with many IT solutions, cloud computing comes in a few different solutions, and the solution that a company selects will have important ramifications on the business and legal issues it must consider. "Private clouds" offer a dedicated hardware environment for the customer that is not shared with any of the vendor's other customers. This model offers more modest economies of scale, but nonetheless provides many of the same scaled-resource capabilities offered by public clouds. In certain cases, the private cloud customer also can dictate in which country (or countries) its data will be hosted. This allows a customer to avoid situations where its data is being hosted in a country that the customer considers high-risk (*e.g.*, for security or regulatory reasons). "Public clouds," in which resources are provided on a shared, self-service, "pay-as-you-go" basis, can deliver the best economies of scale, but the shared infrastructure model can limit customization and may not offer adequate security for customers storing highly sensitive data. "Hybrid clouds" are a combination of public and private clouds in which users protect their most highly sensitive information on a private cloud but store less critical data on the vendor's public cloud. This allows a customer to take advantage of the security of a private cloud when necessary and enjoy the cost savings of a public cloud when appropriate.

Data Protection

The first issue that companies need to consider when determining whether to use cloud computing is security. Most security experts note that cloud computing provides an enticing target for hackers since so many different companies' data may be stored in a single location. In addition, since security only is as strong as the weakest link, grouping companies together may mean that all are exposed to the security protections of the weakest customer. In general, companies should analyze carefully the type of data they plan to store in a cloud, and whether the security protocols followed by the cloud

If you have any questions regarding the matters discussed in this memorandum, please contact ***Stuart D. Levi*** *at 212.735.2750, stuart.levi@skadden.com or call your regular Skadden contact.*

* * *

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

provider meet the company's vendor requirements. While cloud providers can tout a more secure environment than those offered by their customers, they often are making this comparison against small or mid-sized companies that cannot afford robust security protection on their own. Large companies may find that the security offered by certain cloud computing providers fall short.

Jurisdictional Issues

Companies also need to consider the jurisdictional issues presented by cloud computing. Unless the company uses a private cloud solution in which it can specify where its data is to be stored, companies should expect that their data may be stored in countries where they currently do not do business. As a result, potential cloud customers often question whether using cloud computing will mean that they are "doing business" for jurisdictional purposes in all countries where their data is being stored. To date, no court has addressed this issue, and it would seem difficult to find that a company is doing business in a jurisdiction simply because a third-party vendor is storing its data in that country.

The jurisdiction issue that has received the most attention has been the potential application of the U.S. Patriot Act to foreign companies that use a U.S. cloud provider. The argument is that under the Patriot Act, the U.S. government has the authority to subpoena data from any entity that has (i) "minimum contacts" within the U.S. sufficient to establish personal jurisdiction; and (ii) "possession, custody or control" of the data in question, regardless of whether such data is located within the U.S. or elsewhere. The use of the "possession, custody, or control" terminology is viewed by some as giving the U.S. government broad latitude to subpoena cloud data stored in the United States. Their argument is that a cloud provider located in the U.S. satisfies the minimum contacts test and has possession of data (even though the data belongs to the third party).

The power afforded the U.S. government under the Patriot Act is not unlimited. Governmental authorities only may access data pursuant to the Patriot Act to (i) "obtain foreign intelligence information not concerning a United States person;" or (ii) "protect against international terrorism or clandestine intelligence activities." Therefore, the Patriot Act may not be used as a means to access data for the purpose of simply investigating business activities. Moreover, the U.S. State Department has stated that the risk that the U.S. government would obtain cloud-based data through the Patriot Act has been overstated. Indeed, many argue that this concern has been raised by non-U.S. cloud providers to provide themselves with a competitive advantage. Nonetheless, the U.S, government has yet to take a definitive stance on this issue. To that end, a 2011 cloud computing report signed by a coalition of 71 experts from companies such as Microsoft and Amazon has urged the Commerce Department to conduct a study of the Patriot Act in relation to cloud computing.[1]

Overall, cloud computing can provide companies with significant cost-savings and efficiencies. However, unlike other IT solutions, cloud computing can present legal risks that should be carefully considered with the company's legal department or outside legal counsel.

---

1 To download a copy of the report, visit http://www.techamericafoundation.org/cloud-commission.