TEXAS LAWYER

An ALM Publication

texaslawyer.com | June 13, 2018

Commentary

Considerations for Cloud Computing Agreements

When negotiating agreements with cloud service providers, it is important to know how cloud computing works, the risks associated with cloud computing and how these risks should be addressed, and the type of support that the business will need on an ongoing basis.

BY JILL A. MCWHIRTER AND RAJESH D. PATEL

Cloud computing is a subscription-based service where a person or business can obtain networked storage space and computer resources for a fee. There are different types of cloud computing services. The two most popular types of cloud computing services are Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS). In an SaaS offering, enterprise applications and associated data are hosted on the cloud service provider's servers and storage systems. Users gain access to SaaS enterprise applications and associated data using a web browser and typically pay a fee per user per month. In an IaaS offering, the provider provides the infrastructure components to a user, which includes on-premise servers, virtual machines, storage devices, and networking resources to run the enterprise applications on a pay per use basis. The company or user is responsible for installing and maintaining the operating system and application or virtual machine, while the provider is responsible for managing the infrastructure hardware that the applications or virtual machines run on.

Photo: Brian Jackson – Fotolia

Cloud computing involves delivering hosted services over the internet. The service end is where the data or software is stored and the user end is a single user or company network. Thus, users would turn on their computer, connect to the web and to the servers holding their data, click on the application software, and then just start using the application with the data that is stored at the service end.

There are many benefits to cloud computing, which explains why so many people

and companies are turning toward cloud computing. Many of these benefits relate to cost savings, flexibility and efficiency. First, cloud computing minimizes the hardware, such as memory, and application requirements, such as word processing, for the users and pools those resources in the cloud, thereby minimizing costs. Second, there is a greater flexibility for companies in ramping up and down their capacity requirements depending upon the business needs, e.g., peak and non-peak times of the year, without incurring costs for massive data storage and expensive servers. Third, businesses are able to refresh aging infrastructure without incurring capital expenditure costs. Newer technologies may require more powerful and resilient servers in which companies can use cloud computing without having to invest in new servers to accommodate their new technologies. Fourth, businesses can increase productivity since a user can access data and applications from anywhere rather than from a specific location where the data may reside. Further, cloud computing frees up IT staff up for other projects since many cloud computing providers often offer infrastructure as well as management services. These are just some of the many benefits of cloud computing.

When negotiating agreements with cloud service providers, it is important to know how cloud computing works, the risks associated with cloud computing and how these risks should be addressed, and the type of support that the business will need on an ongoing basis. The company's valuable assets will be in the hand of a third-party service provider.

Some "watch-outs" to be aware of during these negotiations include the following:

- Ensure that all data uploaded by the company or any of its affiliates are owned by the company, and not the service provider, regardless of whether the data has been modified by the service provider.
- Ensure that all data stored by the service provider is only for the use of the company and its affiliates and that the service provider is prohibited from monitoring the company's data usage or using any information related to the data for any purpose other than providing services to the company.
- Determine where each of the service provider, the data centers, any back-up data centers, the service support call center, and any other third party that may have access to the data is located for ensuring compliance with local and export laws.
- Consider the type of data that will be stored in the cloud.
- Determine the security level of the service provider in protecting the data while in storage and during transmission.
- Determine the procedure that the service provider will use in the event of a breach and that the service provider will notify the company.
- Determine the mechanisms to provide for disaster recovery and business continuity procedures in the event of disaster.
- Determine the types of liability, the amount, and the limitations of liability that the service provider is willing to take on.
- Determine the technical support and service levels that the service provider is offering.
- Address choice of law, venue and dispute resolution mechanisms.
- Ensure that there is adequate time to "leave the cloud" and transfer data back to company or another provider in the event that the agreement is being terminated.

Jill A. McWhirter, *a partner in King & Spalding's intellectual property counseling practice in Houston, specializes in identifying and solving cutting-edge intellectual property issues in complex transactions in the energy and technology sectors. She can be reached at jmcwhirter@kslaw.com.*

Rajesh D. Patel *is counsel with the corporate, finance and investment group practice in the firm's Houston office. His practice focuses on intellectual property, primarily in transactional issues regarding patent, trademark, copyright, licensing and due diligence, along with litigation support. He can be reached at rdpatel@kslaw.com.*