Insights into Cloud Computing

W. Michael Ryan

June 4, 2010

The Basics

The basic point of cloud computing is to avoid acquiring and maintaining computer equipment and software while at the same time increasing the ease-of-use and flexibility of the benefit offered by the technology.

Cloud computing allows computer technology to be easily accessed as a service over the Internet or via a private network from any location, so that computer infrastructure, programs and data can be available when and where the user needs them.

The enterprise only pays for as much data processing as it needs, avoiding the capital expenditure and the ongoing expense of maintaining the infrastructure. The same concept applies to the software application, thereby avoiding the upfront license fee and ongoing cost of supporting the software.

Flexible pricing on a pay-for-use basis is a big piece of the value proposition, along with the rapid increase and decrease of usage with minimal involvement by the service provider. Rather than buying and maintaining server capacity and operating systems, an enterprise can acquire that same capability from a cloud provider and access it over the Internet.

Common Definitions

The term "Cloud Computing" has caught fire and is used for advertising and in the media in a variety of contexts. The Commerce Department's National Institute of Standards and Technology (NIST) has attempted to provide some structure to the cloud computing conversation with some helpful definitions. NIST defines three basic types of service models for the cloud:

- **Cloud Infrastructure as a Service (IaaS)**, involving the provisioning of computer infrastructure.

- **Cloud Software as a Service (SaaS)**, involving access to a provider's software applications.

- **Cloud Platform as a Service (PaaS)**, involving accessing a software development environment.

These service models can be deployed in four ways. "Private clouds" are where all the technology components, servers and software, as well as software development, are kept in-house. This way an enterprise makes better use of its current assets; for example, not every laptop has to be loaded with the software and have the data stored on it. These private clouds are increasing being deployed within larger enterprises.

A "public cloud" – such as salesforce.com, Amazon's cloud offering or Gmail – is available to anyone. This deployment model offers the greatest potential flexibility and savings but also involves giving the service provider the greatest control over the enterprise's technology capabilities. Many large enterprises are using this deployment for discrete services and are evaluating ways to further utilize the model.

The service models may also be deployed using a "community cloud", which NIST defines as multiple organizations that have shared concerns around things like security, privacy, or regulatory compliance. An example could be the healthcare industry, or even more narrowly, hospitals.

The fourth delivery model is a "hybrid cloud" which involves an interface between two or more of the three preceding models.

Overview of Issues

Deploying a cloud computing service model offers significant benefits to an enterprise, but also involves a need to carefully evaluate and manage the business and legal risk. Many enterprises are in the process of weighing the potential benefits against the potential risks, particularly with regard to public clouds. The following are some of the key points to consider in evaluating a cloud computing deployment.

Contractual Terms

In many ways, the contractual issues faced in moving to a public cloud are not any different than those faced by an enterprise using a traditional technology outsourcing business model.

However, traditional technology outsourcing typically involves both customization of the solution being delivered for a particular customer and ongoing control of the service provider's delivery of the solution, particularly at the large enterprise level. In almost all cases, the data and information of the outsourcing customer will be stored, process and transmitted in a pre-defined manner and at known locations. This customization of the business and technology solution and ongoing control are in tension with the basic value proposition offered by cloud computing.

Quick and efficient contracting processes are often sought but frequently realized in complex relationships involving enterprise operations. Alternative contracting process and standards may evolve to assist in achieving the efficiency and ease-of-use promise of cloud computing. In the interim, large enterprise customers are likely going to need to spend time carefully considering and, to the extent possible, negotiating the contracts governing their significant public cloud deployments.

Some of the key areas that need to be addressed by the cloud computing contract include:

- A clear articulation of fees for base services and modifications over time.

- Well-defined performance metrics and remedies for service failures, and an understanding of how the metrics may change over time.

- Security, privacy and audit commitments that will satisfy regulatory concerns, including an understanding of where data and information (including intellectual property) resides.

- Adequate provision for termination of the contract and moving to a substitute provider.

- Understanding the process for changes to the solution over time and the impact on connections between the cloud solution and other systems and processes utilized by a customer.

- Addressing business continuity, disaster recovery and *force majeure* events.

- Clear restrictions on use and ownership of customer data and any intellectual property of the customer resident in the cloud.

- A reasonable allocation of risk for breaches of contract and for third party claims related to the solution.

- Understanding subcontractors that may be used by the service provider.

- Addressing the resolution and impact of disputes and bankruptcy.

Regulatory Constraints

The major issues that an enterprise or its counsel must be aware of when acquiring public or private cloud computing capacity vary by industry and the regulatory regimes applicable to the enterprise. For instance, a financial institution has the requirements of Gramm-Leach-Bliley (GLB) and cannot move to public cloud until it is comfortable the privacy and security standards are compliant and that its regulators will agree. Institutions covered by the Health Insurance Portability and Accountability Act (HIPAA) will have similar concerns to address their requirements with regard to protected health information. In addition the FTC and state attorney generals are focused on the protections accorded personal information in cloud computing environments. The Sarbanes-Oxley Act and Payment Card Industry Data Security Standards may also apply to the use of a cloud computing solution.

E-Discovery

It's unlikely a court would expect a system to be perfect, whether it's in-house or in a cloud. However, a company cannot outsource its responsibility to comply with discovery obligations – it must put in place a reasonable process for data to be retained, preserved and protected. That means a company must understand its ability to cause a cloud service provider to comply with discovery requests. If a company simply signs a form agreement offered by a service provider, it may find itself challenged to defend its actions as reasonable if it cannot produce documents as required in litigation.

Cross-Border Issues

Every company will need to understand the jurisdictions in which its data and confidential information may be stored . These laws and governmental policies may make the data and information more or less vulnerable to being accessed by governmental authorities and private parties.

Mike Ryan, a Partner in Kelley Drye's Chicago office and chair of the firm's Technology Transactions and Sourcing Group, represents health care companies, consulting firms, financial services companies and clients in many other industries. He has extensive experience advising on transactions with an international scope, including working with Kelley Drye's independent affiliate office in Mumbai, India.

The types of matters in which Mike has been involved include outsourcing (both IT and business process); software development and implementation; intellectual property licensing; mergers, acquisitions, joint ventures and other strategic alliances; and equity investments.