This article was originally published in the November 2010 issue of the Intellectual Property & Technology Law Journal.

Insights into Cloud Computing

The basic point of cloud computing is to avoid acquiring and maintaining computer equipment and software, 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 technology, software programs, and data can be available when and where the user needs them.

The customer only pays for as much technology capacity as it needs. For computer processing, a company using cloud computing can avoid the capital expenditure and the ongoing expense of maintaining the computer infrastructure. The same concept applies to the software application, allowing the company to avoid the upfront license fee.

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 or paying upfront licensing fees, an enterprise can acquire that same capability from a cloud provider, access it over the Internet, and pay a pre-defined price for the service.

This article examines the contracting issues relating to public cloud computing, as well as the privacy, data security, and e-discovery considerations for customers investigating public cloud computing alternatives.

Common Definitions

The term “cloud computing” has caught fire and is used in a variety of contexts in advertising and the media. The Commerce Department's National Institute of Standards and Technology (NIST) has attempted to provide structure to the cloud computing conversation with some helpful definitions.[1] NIST defines three basic types of service models for cloud computing:

- *Cloud Infrastructure as a Service (IaaS),* involving the provisioning of fundamental computer resources (*e.g.*, processing, storage, networks);
- *Cloud Software as a Service (SaaS),* involving access to a provider’s software applications running on a cloud infrastructure; and
- *Cloud Platform as a Service (PaaS),* involving the provision to users of the capability to deploy onto the cloud infrastructure applications created by the user with provider-supported programming languages and tools.

The NIST describes four models for deployment of the cloud infrastructure. *“Private clouds”* maintain all the technology components, servers, and software for a single organization. The solution may be managed by the user or a third party but is provided for the benefit of only one organization. The customer 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 increasingly being deployed within larger enterprises.

A “*public cloud*,” such as *salesforce.com*, Amazon’s cloud offering, or Google’s gmail, is available to anyone or to large industry groups and in either case is owned by the provider of the service. This deployment model offers the greatest potential flexibility and savings but also involves granting 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 use the model.

[1] *See http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc*.

The service models may be deployed using a "*community cloud*," which NIST defines as cloud infrastructure shared by several organizations and that supports a specific community that has shared concerns. The shared concerns could be the mission of the organizations or security, privacy, policy, or regulatory compliance.

The fourth delivery model is a "*hybrid cloud*," which involves a composition of two or more of the three preceding models.

Overview of Contracting Process and Issues

Pre-Contract Evaluation

Deploying a public cloud computing delivery model offers significant benefits to a customer 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 of implementing cloud computing against the risks. As a preliminary matter, a customer should carefully analyze potential uses for cloud computing from a business, technology, and legal/regulatory perspective and determine those areas where the cost savings justify moving to an IaaS, SaaS, or PaaS model and those where the risks are too high.

However, even for very commoditized applications, a customer will need to carefully consider issues related to the data resident within the applications. For example, the e-discovery and document retention policy issues described below are particularly important with regard to the use of a cloud computing solution for e-mail.

Experience of Customer

In many ways, the contractual issues involved in moving to a public cloud are not much different from those faced by an enterprise in obtaining technology solutions using existing delivery models. A customer entering into an IaaS arrangement must address the same basic set of issues that a customer entering into a traditional infrastructure outsourcing agreement addresses, although the IaaS service model may result in the issues being addressed differently.

Similarly, customers entering into a SaaS agreement must address the same issues as a company using an application service provider (ASP) model to acquire the use of software. However, while most companies are very familiar with infrastructure outsourcing and hosting arrangements, many are not as familiar with ASP models. The traditional software licensing approach is still much more common than acquiring software as a service. As a result, the SaaS contract is likely to be a newer experience from a contractual standpoint than an IaaS solution.

Traditional infrastructure outsourcing, and even some ASP models, involved both customization of the solution being delivered for a particular customer and some level of ongoing control over 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 is stored, processed, and transmitted in a pre-defined manner and at known locations under pre-cloud computing models.

However, the customization of the business and technology solution and ongoing customer control present in traditional outsourcing transactions are in tension with the basic value proposition offered by cloud computing. Regardless of the service delivery model, the cloud computing provider's business model is predicated on providing a common solution to multiple customers and retaining the ability to maximize the use of the provider's technology assets in servicing those

clients. This business model drives the vastly lower pricing offered as compared to a traditional information technology outsourcing but also requires that the provider maintain a higher level of control of the solution.

From the provider's perspective, the cloud computing model implies a simpler and straightforward contracting process than is typical with pre-cloud computing arrangements. However, quick and efficient contracting processes have often been sought in a variety of business arrangements but are infrequently realized in complex relationships involving enterprise operations. Alternative contracting processes 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 spend time carefully considering and, to the extent possible, negotiating the contracts governing their significant public cloud deployments.

Comparisons to Traditional Contracting Models

Under more traditional outsourcing agreements, a large customer could require the service provider to customize the solution to meet the customer's specific needs around areas such as disaster recovery/business continuity, record retention/destruction policies, project staff requirements (including backgrounds checks and drug testing), and service level requirements. A customer of a cloud computing offering can expect less flexibility around these types of policy and operational matters.

On the other hand, there are some areas in which the business model behind cloud computing could result in more favorable provisions for the customer than in traditional outsourcing. For instance, minimum payments and termination charges under a traditional outsourcing arrangement are justified by reference to the upfront investment by the service provider and the cost of demobilization. These costs should be minimal in a cloud computing environment, leaving the provider to justify provisions related to a minimum term of the agreement, minimum payments (or exclusivity), and termination charges based almost exclusively on more favorable pricing than if these terms were not included.

As another example, providers of traditional information technology services have rarely agreed to most-favored-customer provisions on the basis that comparing one customer to another customer is very difficult. With a more standardized cloud computing offering, customers may push harder for this type of protection both with respect to pricing and to service levels and associated service level credits.

While the risk allocation provisions (*e.g.*, indemnities, representation and warranties, limit/exclusions of liability, and related exceptions) in cloud computing agreements are not directly tied to the cloud computing operating model, providers are more aggressive in asserting that the significantly reduced price reflects a standardized allocation of risk. Top-tier customers will, however, continue to push for the providers to agree to risk allocation provisions consistent with those used in more traditional outsourcing arrangements.

Even if the contract provides for reasonable termination assistance, for some cloud computing offerings it may be very difficult as a business or technical matter for the customer to migrate to another provider. In those cases, the customer will have an increased need for the provider to commit to continuous improvement of the service and assurances that the pricing remains competitive over time. In addition, for SaaS and PaaS offerings, customers will have the same concerns related to improvements to the functionality of the software (or removal of functionality) as with traditional software licensing arrangements.

Checklist of Contractual Issues

The following is a list of some of the key areas that need to be addressed by the cloud computing contract:

- 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) reside;

- Clear delineation of the affiliated entities that may receive services under the contract as well as provision for the continued receipt of services by divested entities during a transition period;

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

- Adequate provision for termination of the contract and moving to a substitute provider, including termination assistance and recovery of all data;

- 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;

- Access and recover of customer data as needed and an understanding of the customer's rights with regard to litigation holds and e-discovery requirements;

- 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 and the conditions for the service provider using subcontractors; and

- Addressing the resolution and impact of disputes and bankruptcy (*e.g.*, software escrow arrangements for SaaS offering).

Intellectual Property Rights

In an IaaS environment, the customer will need to clearly provide in the agreement that, as between the provider and the customer, the customer maintains all intellectual property ownership rights related to any applications that it runs using the IaaS platform. Of course, reasonable confidentiality provisions will need to be included to protect any trade secrets that the customer places on the IaaS platform. The obligations to acquire third-party consents should also be straightforward in the cloud computing environment, with the provider being responsible for any consents required for it to operate its solution and the customer acquiring necessary third-party consents required in connection with any application or data that the customer brings to the public cloud platform.

The intellectual property and licensing structure for an SaaS and PaaS solution could be more complex, depending on the intellectual property at issue. The provider will retain ownership of its solution, but the customer will need to consider the ownership of any intellectual property for any interfaces or add-ons that the customer develops in connection with using the services as well as the ownership of applications developed on a PaaS platform. The customer will likely lose the ability to control any new processes, methodologies or approaches that it wishes to see incorporated into the SaaS or PaaS solution by the provider and may have difficulty implementing new approaches without the cooperation of the provider. The issues related to maintaining proprietary ownership of intellectual property versus releasing intellectual property into a community will need to be carefully considered prior to implementing a SaaS or PaaS solution.

Disaster Recovery/Business Continuity

In the disaster recovery/business continuity and document retention area, the contract will, at a minimum, serve to document the current policies of the cloud computer provider as well provide for the customer to receive notices of changes and updates. For disaster recovery/business continuity, the customer will also need to seek assurances that

adequate testing is done on a regular basis and define the customer's ability to monitor and participate in the testing. One of the benefits of a cloud computing environment should be enhanced ability of the provider to rapidly recover from any outage and to greatly reduce the down-time.

Compliance with Laws

The customer will also need to consider the commitments the cloud computer provider is making with respect to compliance with laws at the outset of the contract. The provider should be willing to contractually agree that it is complying with laws generally applicable to its business. The customer will need to assure itself that it will remain in compliance with laws applicable to its business upon commencement of the cloud computing offering.

As with traditional outsourcing and software licensing arrangements, addressing compliance with changes in laws over time can be problematic depending on the laws applicable to the delivery and receipt of the cloud computing services. Providers of cloud computing offerings tailored for specific regulated industries may agree to modify their offerings to address changes in laws over time. In any event, a regulated customer will need to conclude that it is able to maintain its compliance with laws and will likely also need to develop a reasonable plan for migrating off the cloud computing platform if necessary to comply with changes in laws that are not addressed by the provider's offering.

Audit Rights

A customer using a cloud computing solution will need to review its audit rights in the agreement and confirm that they are adequate for the customer's regulatory compliance needs. Most large customers will likely seek to obtain the same audit rights as in more traditional information technology outsourcing, with respect to both the services and the fees. However, cloud computing providers are unlikely to agree to audit rights for all but a few customers given the potential disruption of such audits and the need to carefully restrict any access to the data of other clients. At a minimum, customers will need to obtain industry standard certifications as to the adequacy of the internal controls of the provider (such as SAS 70 Type 2 audits) and must insist on the ability of the regulators to conduct audits of the provider as may be required by such regulators.

A complete understanding of the data and document retention and destruction policies of the cloud computing provider, both at the time of contracting and during the term of the agreement, is also critical to understanding the information that may be available to an adversary during the litigation process.

Privacy and Information Security

When acquiring public or private cloud computing capacity, a company must be aware of privacy and information security issues. Certain privacy and data security obligations may arise from several sources, including contractual obligations and regulatory requirements.

Privacy & Data Security Contractual Obligations

Privacy and information security obligations may originate from contractual commitments made to end-users and business partners, such as representations and promises made in a privacy policy. These promises may range from whether and how the company shares customer information, the level of security provided to such stored information, and the types of service providers with whom the company shares customer data and for what purposes. If any of these representations in the privacy policy (or others) conflict with a company's use of cloud computing, before the company can roll out the cloud services, it may need to update its privacy policy to address the new business practices to keep the privacy policy accurate. Depending on the change, this may be a material change that could trigger additional notice and consent obligations for the company before applying the updated policy.

Additionally, a privacy policy typically summarizes at a high level how a company protects customer data. To confirm the accuracy of such safeguard representations, a company often needs to take certain due diligence and contractual

measures with any third parties with whom it shares customer data to confirm that the parties will protect the data as well. Thus, when acquiring cloud computing capacity, a company will also need to conduct appropriate due diligence of the cloud computing service provider's privacy policy and data safeguards. The contract between the company and the cloud computing service provider often will address issues such as:

- A specific description of how the provider will safeguard customer data stored;
- The process for the service provider to provide notice to the company if the provider suffers (or may have suffered) a data breach;
- If feasible, obligations to keep the company's data logically separate from other data; and
- Confirming that the cloud computing services comply with promises the company has made to its customers.

Further, if a company allows its customers to make purchases with payment cards, the company is likely contractually bound to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). This obligation is usually contained within the merchant agreements executed by the company and the various payment card brands. If payment card information will be stored in the cloud, to remain PCI DSS compliant, a company will need to ensure that its service providers are PCI DSS compliant.

Privacy & Data Security Regulatory Requirements

In addition to contractual obligations, a company should be aware of privacy and data security obligations imposed by regulatory requirements. The specific regulations applicable to an enterprise often can vary by industry, although certain baseline principles are applicable to all enterprises that collect, use, store, or share customer information. For instance, the Gramm-Leach-Bliley Act (GLB Act) regulates the privacy and information security practices of financial institutions, including the obligation to provide certain disclosures in annual privacy statements to customers and to protect customer information in a manner consistent with the Safeguards Rule. Institutions covered by the Health Insurance Portability and Accountability Act (HIPAA) similarly should address regulatory requirements with regard to protected health information.

Further, even companies that are not subject to industry-specific regulatory requirements are subject to the Federal Trade Commission's (FTC) general authority to prohibit unfair or deceptive acts or practices under § 5 of the FTC Act. When evaluating a company's privacy and information security practices, the FTC often focuses on whether the company accurately represented how it handles personal information in its privacy policy and/or whether it failed to implement "reasonable" and "appropriate" controls to secure sensitive personal information in a way that causes, or is likely to cause, substantial consumer injury that is not outweighed by benefits to consumers and where the injury is not reasonably avoidable by consumers. As a baseline matter, before implementing cloud computing with consumer information, a company should ensure that its practices are accurately described and that service providers can provide reasonable and appropriate protection of such information based on the size and complexity of the company, the nature and scope of the company's activities, and the sensitivity of the information.

State laws and regulations may also affect a company's determination of whether and how to use cloud computing services. For example, Massachusetts has enacted robust regulations that govern safeguards applied to Massachusetts residents' personal information. Additionally, Nevada has enacted a law that requires compliance with PCI DSS for payment card information and establishes specific requirements regarding the encryption of other personal information. Further, Washington and Minnesota have codified elements of PCI DSS and permit financial institutions to seek damages from businesses and payment processors that fail to provide reasonable protection of payment card information when such failure is determined to be the proximate cause of a security breach. Other states' laws impose general safeguard and contractual requirements with respect to the protection of personal information. Thus, careful consideration of a cloud computing provider's safeguard practices is warranted, given the potential exposure that a company may face in relation to the personal information that it stores and accesses in the cloud.

Additionally, a company will need to be aware of how international law may restrict the use of cloud computing services. For many cloud computing services, customer data may be replicated and/or separated into small portions and stored on multiple servers. If data is sent across international boundaries, privacy and data security concerns related to such cross-border data can be triggered.

For example, privacy and data security laws implemented by European countries pursuant to the EU data protection directive restrict the transfer of EU citizens' personal data outside the European Union.

Personal data may be transferred outside the European Union only if the recipient is located in a country that can provide an adequate level of protection. Currently, US data protection laws do not meet the EU standard. To transfer personal information from the European Union to the United States, a company must be certified under the US-EU Safe Harbor. Other restrictions apply depending on the country at issue, particularly in light of the fast evolving nature of privacy laws around the globe.

It is important for a company to know where these servers are located and whether the cloud computing service provider offers the capability to limit the transfer of data across specific or all international boundaries.

E-Discovery

Courts will likely not expect any data retrieval system to be perfect, regardless of whether it is provided in-house or in a cloud. However, a company would be remiss in trying to outsource its responsibility to comply with discovery obligations; it must put in place a reasonable process for data to be retained, preserved, protected, and disclosed.

There are currently no universally accepted standards that cloud computing providers must follow in storing and maintaining information, although various groups are looking to develop them. Since the cloud computing provider is generally not going to be a party to the litigation, if a company cannot disclose the required electronically stored information, the company, not the cloud computing provider, is subject to sanctions. Courts have accessed high penalties and sanctions for spoliation of information where potentially relevant information is lost.[2]

The time to consider the issues associated with e-discovery requests is during the due diligence and contracting process with the cloud computing provider. Dealing with these issues for the first time when litigation holds are being issued could prove very challenging at best and, at worse, disastrous from a litigation perspective.

* * *

Ryan, W Michael; Loeffler, Christopher M. Intellectual Property & Technology Law Journal**; Clifton** Vol. 22, Iss. 11, (Nov 2010): 22-28,1.

[2] *See, e.g.,* United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21, 26 (D.D.C. 2004) (sanction of $2.7 million for spoliation).