MAYER·BROWN

Article
September 2010

Clear Skies or Stormy Weather for Cloud Computing: Key Issues in Contracting for Cloud Computing Services

By Rebecca S. Eisner and Daniel Masur

Cloud computing has been with us for years through technology outsourcing, online service models and application service providers. But an entirely new crop of providers and service offerings has changed the way customers are contracting for cloud computing services. This article addresses cloud computing benefits, risks and regulatory challenges, with suggestions for overcoming or mitigating those challenges.

What Is Cloud Computing?

While there is no universally accepted definition of cloud computing, most agree that there are three service models, each with its own distinct features: software as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS). There are also different delivery methods: a "private cloud," where the resources used to provide the services are dedicated to one specific customer; a "public cloud," where the resources are shared generally with the provider's other customers; and a "hybrid cloud," where multiple clouds (of the same or different types) are interconnected—for example, the majority of an entity's processing may be performed in a private cloud but it may access data shared on an application in a public cloud.

While the definition of cloud computing may vary, there is agreement on its benefits. There are technical advantages: the user gets on-demand computing services; computing resources such as storage, processing, memory, network and bandwidth are pooled across multiple users; and fluctuations in demand are more easily met. There are also time- and money-saving advantages as customers do not have to invest in the hardware, software and network infrastructure needed to provide the same service. Cloud computing also increases the opportunity for collaboration and knowledge sharing, as all files are available to designated users in a consistent format. Also, cloud computing services are available over a network, so they can be accessed from many locations.

The Current State of Cloud Computing Contracting

Currently, the standard contracts offered by cloud computing providers are one-sided and service provider-friendly, with little opportunity to change terms. Few offer meaningful service levels or assume any responsibility for legal compliance, security or data protection. Many permit suspension of service or unilateral termination, and disclaim all or most of the provider's potential liability. In addition, some cloud computing providers emphasize low cost offerings, which leave little room for robust contractual commitments or customer requirements.

When contracting for these services, it is critical for a business to analyze its data, applications and business needs. Routine, non-sensitive data may

allow use of a standardized, low-cost cloud computing service with few contractual protections. However, mission critical data and applications require more robust service and contractual protections, which may increase the price of the service.

In those situations where standardized services and terms are not appropriate, where can business lawyers look for appropriate contractual protections? While there is no single form agreement that properly addresses all contractual needs, there are some good starting points. Traditional outsourcing and software licensing terms may be useful in creating an appropriate set of contractual clauses. These terms will need to address the regulatory and compliance challenges discussed below.

Potential Operating Risks of Cloud Computing

On the operational side, cloud computing relies heavily on network connectivity. If network connections are down, or slowed, the resources and data in the cloud can become unavailable. This risk is heightened with public and hybrid clouds where resources are shared, not dedicated. Depending on the nature of the cloud, resources that are supposedly abundant may in fact be heavily used and, therefore, less available. Another operational risk exists because of the lack of standards in cloud computing: there may be compatibility issues between the cloud and data and resources in a different cloud, or elsewhere in the customer's enterprise .

As with traditional outsourcing, a number of risks center on the fact that the business is giving up control. This lack of control can undermine many of the benefits sought from cloud computing as well as pose other risks to the business. The customer may need a change in the service to accommodate a new customer regulatory requirement. The cloud provider may not be willing to make the change if it costs money or changes a standard service. Gaining control of these issues in the contract with a cloud provider can increase the cost of the solution, and may reduce some of the cost benefits of using a cloud computing solution.

Regulatory and Compliance Challenges

There are a number of regulatory challenges for cloud computing users and providers. This article gives a few examples, but does not address every regulatory concern. For example, businesses involved in government contracting often have obligations to classify and protect data. Restrictions on data disclosure and access, even on the location of data storage, will have to be considered in the context of any cloud computing solution.

The free movement of data among networks, data centers and storage devices may raise issues under a country's import/export control regulations. For example, a company using cloud computing services may not be aware that its export-controlled software is being exported through its use of the distributed cloud computing system.

Data retention and disposal requirements can also be challenging. For example, in the United States, when litigation is pending, threatened or anticipated, a party must preserve potentially responsive data in the form in which it was created by the company. Such data may have to be made available to the opposing party or the court as required by electronic discovery rules. It could be challenging to isolate and provide data in the cloud given the distributed and disbursed nature of cloud computing.

Privacy and Security Issues: The Largest Of The Regulatory Challenges

Regulated personal information presents one of the largest challenges for cloud computing users and providers. Numerous industry sector specific privacy laws exist that must be addressed in cloud computing contracts. These include, for example, the Gramm-Leach-Bliley Act ("GLB") for privacy financial information, and the Health Insurance Portability and Accountability Act and

implementing regulations (collectively, "HIPAA") for health and medical information. The Federal Trade Commission ("FTC") has devoted significant attention to privacy issues, and security and prevention of identity theft have become a particular focus. The States have also taken notice of privacy and security issues, and have begun enforcement of such issues.

Many states have statutes and regulations that mirror the requirements of GLB and protect personal health information like HIPAA. Additionally, many states have passed data breach notification laws. As of April, 2009, the majority of states, the District of Columbia, Puerto Rico and the Virgin Islands had enacted some form of database breach notification act protecting personal information. Additional state laws are presenting issues for cloud computing regulatory compliance as well. In 2008, Massachusetts issued comprehensive regulations requiring that personal information be encrypted when transmitted wirelessly or over a public network. The regulations also require a "written, comprehensive information security program." The security program must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing personal information.

Finally, there are industry specific standards that many businesses must follow, such as the Payment Card Industry (PCI) Security Standards. Companies that put cardholder data in the cloud will have to ensure that cloud providers also comply with PCI standards.

Europe and other parts of the world have stringent privacy regulations that in many cases have been in place much longer than those in the U.S. In many countries, personal data cannot be processed without the consent of the data subject. Additional requirements include limiting the use of the data to the reason for which is was collected (and the consent granted), allowing the data subject access to his or her personal data and allowing the data subject to correct personal data. In addition, some countries regulate the transfer of personal data (e.g., the European Union Directive 95/46/EC, as implemented through Member State legislation, relating to collection, use, processing and free movement of personal data). Failure to comply can lead to fines, penalties, interruption of business and, in some cases, imprisonment.

Regulatory and Compliance Issues with Cloud Computing: Managing the Risk Through Contracting

To manage privacy risks with service providers, a company must have regulatory, security and privacy processes in place with specific requirements pertaining to service providers. At a high level, these steps include: appropriate service provider diligence and selection; implementing regulatory, security standards and privacy requirements through appropriate operational requirements and contractual clauses; and monitoring performance and adherence to the standards and process.

Businesses that use cloud computing solutions where personal information will be collected, processed, accessed, stored or transferred must perform due diligence on the service provider at the contracting stage, as well as continue meaningful oversight during the term of the contract.

And, while you cannot outsource responsibility for your compliance obligations, you should ensure that you and your provider understand the following topics (and have documented such understanding in the contract):

- The specific regulatory requirements to be performed by your service provider (with respect to privacy, for example, including how the service provider may and may not use personal information, confidentiality terms, how the provider should dispose of personal information, where data may be processed, stored and transferred, etc.);

- Your compliance and security requirements and the service provider's security practices to monitor and prevent compliance and security breaches and to protect your business;
- The process for reviewing any process or system changes that may impact compliance, security or privacy issues;
- Your reporting requirements for regulatory compliance;
- Your audit requirements;
- Your rights to approve any subcontracting by your primary service provider and requirements that subcontractors of all tiers agree to the same compliance terms;
- What you will do if your service provider suffers a security/privacy breach or lapse in compliance, including business continuity and disaster recovery plans;
- Responsibility for monitoring changes in applicable laws and regulations, and adjusting service requirements to meet such changes;
- Liability for breaches of laws, regulation and/or contractual compliance requirements; and
- Of the regulatory compliance requirements, which parts will be provided as part of the services, and which requirements may result in extra charges by the service provider.

Conclusion

Cloud computing offers benefits as well as risks. As cloud computing is a variation of outsourcing, it should not be surprising that many of the risks are the same as or similar to those in more traditional IT outsourcing. Many of the risks are mitigated the same way: appropriate due diligence up front, strong contractual protections that account for higher risk data and applications, and continued vigilant governance. While businesses may discover many beneficial uses of cloud computing, they will also have to determine which applications and data types are not appropriate for cloud computing unless the provider can modify the solution to meet the business' regulatory and other requirements.

For more information about this article please contact one of the authors listed below.

Rebecca S. Eisner
+1 312 701 8577
reisner@mayerbrown.com

Daniel A. Masur
+1 202 263 3226
dmasur@mayerbrown.com