

The Basics of Cloud Computing for the Uninitiated

March 14, 2011

Designed to offer a higher level of scalability, resilience, availability and cost savings that other forms of computing cannot, cloud computing is becoming an increasingly popular way to obtain computing capabilities and services without a substantial capital outlay. But like any business transaction, it is vital to have a solid understanding of the business and legal risks and rewards associated with it prior to entering into any contract arrangement.

What Is Cloud Computing and What Are Its Benefits?

The “evolving paradigm” of cloud computing, as recently defined by The National Institute of Standards in Technology is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud computing is designed to offer a level of scalability, resilience, availability and cost savings that other forms of computing cannot. For example, cloud computing provides unlimited capacity and protection against technology obsolescence, as well as access on demand from anywhere at any time. These features and other key characteristics of cloud computing minimize or even eliminate the need for a significant capital outlay to acquire infrastructure or on-site software applications and in-house IT resources by providing on-demand self-service, broad network access, resource pooling, rapid elasticity and “metered” service. Put simply, cloud computing is a “pay as you go” model of computing.

What Are the Types of Cloud Computing Arrangements?

Generally, cloud computing is provided under three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The most familiar of the service models is SaaS, which enables the consumer to use the provider’s applications running on a cloud infrastructure remotely hosted by the provider. Thus, the consumer has access to the applications via the internet managed by the provider without having to acquire and host the software or the systems required to operate it. The second type of service model, PaaS, allows the provider to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, but does control the deployed applications, and possibly application-hosting environment configurations. The third type of service model is IaaS, in which the provider provides the basic IT infrastructure (*e.g.*,

processing, storage, networks and other computing resources), but the consumer is able to deploy its own operating software and applications, and may control selected networking components (*e.g.*, host firewalls).

In addition to service models, there are also various deployment methods of cloud computing, including public, private, community or hybrid clouds. A public cloud's infrastructure is available to the general public or large industry group and is owned by the cloud service provider, while a private cloud's infrastructure is operated solely for an organization, though it may be managed internally or outsourced to a third party and may be hosted on-site or remotely. A community cloud's infrastructure is shared by several organizations and supports a specific community that has shared concerns (*e.g.*, mission, security requirements, policy and compliance considerations). Health information exchanges or regional health information organizations often employ the community cloud infrastructure. Lastly, a hybrid cloud's infrastructure comprises two or more clouds that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (*e.g.*, cloud bursting for load balancing between clouds).

What Are Some Key Issues to Keep in Mind When Contracting for Cloud Computing Services?

Given the highly technical nature of cloud computing and its emerging use in many regulated industries, such as the financial and health care markets, it is vital to have a solid understanding of the business and legal risks and rewards associated with cloud computing. Like any business transaction, contracting for cloud computing services raises several legal issues that must be adequately addressed in the service contract to ensure an acceptable level of services, to maintain compliance with various federal and state laws, and to provide adequate protections and remedies for both the consumer and the service provider.

The following is a checklist of some key legal and practical issues to consider:

- Data privacy and security safeguards (to ensure compliance with federal and state privacy and breach notification laws, such as the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act and the Gramm–Leach–Bliley Act)
- Intellectual property protection (*e.g.*, adequate protection of proprietary information and trade secrets hosted by the vendor)
- Service level agreements (*e.g.*, 24 hours/7days a week/365 days access, adequate uptime commitments, remedies for chronic downtime, etc.)
- Limitation of liability (and appropriate carve-outs for certain types of claims)

- Indemnity and warranty
- Disaster recovery and business continuity plan (to ensure immediate uninterrupted access despite a disaster)
- Exit strategy (including adequate transition services and retention of data and system access rights in the event of vendor bankruptcy)

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. On the Subject is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

© 2010 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery/Stamford LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, MWE Steuerberatungsgesellschaft mbH, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. McDermott Will & Emery has a strategic alliance with MWE China Law Offices, a separate law firm. These entities coordinate their activities through service agreements. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.