MOSES & SINGER LLP

Technology Bulletin February 2012

Moving to the Cloud: Some Threshold Considerations

Cloud computing promises significant costs savings and more streamlined management of mission-critical information technology, data processing and storage needs. It is now possible to "cloudsource" a wide range of functions, from nuts-and-bolts enterprise email services to complex industry-specific applications.

However, as with all IT outsourcing initiatives, the devil is in the details. From both a business and legal perspective, a customer should engage in a robust due diligence review to ensure that a cloud service provider will be able to meet the customer's financial, operational, legal and regulatory requirements. At the same time, the deal must be structured in a manner that permits the service provider to leverage a fairly standard and scalable offering at a price-point that makes sense. Otherwise, there is a good chance that neither customer nor provider will be happy with the relationship.

What is Cloud Computing?

Cloud computing allows a company to outsource all or parts of its IT infrastructure and convert it to one or more subscription-based services. Under this model, software and customer data are typically located on the vendor's servers and other infrastructure, and the customer accesses that software and processes its data over the public Internet or via a private or semi-private network.

Pricing of the Service. Is it Really Cheaper?

As with all outsourcings, the relationship is not likely to succeed in the long run unless pricing is fair to both parties. The potential economic advantage of transforming a capital expense (e.g., the cost associated with provisioning data centers) into a pay-as-you-go operating expense can become illusory if additional costs must be incurred in order to maintain at least the same level of service enjoyed prior to the outsourcing.

Customer Control Over the Service and Data.

Favorable pricing for a "one-size-fits-all" solution is often accompanied by limitations on an individual customer's ability to control and tailor how the service is provided. However, a customer will usually want to have immediate, reliable and unfettered access to its data, regardless of where or how the data is processed and stored. Customers will also typically require the return of all data upon termination of the contract.

Data Security Breaches

The ease with which data may be moved, processed, stored and accessed globally (including by mobile devices) increases the data's vulnerability to security breach and the corresponding adverse

legal, regulatory and business consequences. A data breach can result in sanctions imposed by regulatory agencies, loss of business, reputational risk, complying with statutory notification obligations and cost of remediation (including credit repair/monitoring for the company's customers).

Service Levels and Disaster Recovery

Service providers usually attempt to minimize their representations and warranties regarding the services, particularly regarding protection against data breaches. Conversely, because a data breach can result in significant adverse consequences, customers will often seek to hold the service provider liable for breaches occurring on its side of the "cloud". Similarly, for service agreements dealing with mission critical data or processes, customers will always want to ensure that the service provider has adequate disaster recovery and business continuity plans in place. Moreover, customers in some regulated industries, (e.g. financial services) are required to maintain business continuity plans in place, and, in turn, ensure that their service providers have such plans as well.

Relocation of Services

Many boiler-plate agreements place no restriction on where the service provider may provide the services or process or store a customer's data. As a result, global providers may be free to service their customers from anywhere in their system. Customers with regulatory or contractual requirements to process and maintain data in certain geographic regions will need to obligate their service providers in a manner that will enable the customer to meet those requirements.

Use of Subcontractors

Customers may require the right to pre-approve a service provider's use of subcontractors, and will want to ensure that the contract holds the provider responsible for its subcontractors' performance.

Modifications to the Agreement; Termination

Some standard agreements authorize the service provider to modify the agreement by posting changes on the provider's website. If the customer continues to use the services subsequent to posting, the customer is deemed to have consented to the change. Customers should seek the right to terminate the agreement in the event that material changes are made to the services. Upon termination of the Agreement for any reason, the provider should be obligated to return the company's data and information in a format that allows for the service to be transitioned back to the company or to a successor service provider.

Compliance with Legal, Privacy and Security Requirements

Moving to the cloud does not relieve the customer of its independent legal and regulatory obligations. For example, the customer will want to be confident that the service is provided in a manner that will permit it to meet its data security, privacy and confidentiality obligations. Applicable laws, regulatory oversight and auditing obligations can vary widely depending on the industry, the types of data being processed and stored, how data flows from one jurisdiction to another and, more generally, where services are being performed and received.

Following is a brief overview of some key laws that may impact the provision of cloud services.

United States

The United States does not have a uniform set of data protection and privacy laws. Rather, a patchwork set of industry-specific laws, regulations and standards have developed over time. Companies that collect, process, store or transmit data may be subject to law and regulation by:

- Federal Trade Commission
- Electronic Communications Privacy Act
- Children's Online Privacy Protection Act
- USA PATRIOT Act
- State Privacy and Breach Notification Laws of 46 states plus Puerto Rico, Virgin Islands and the District of Columbia
- Pending Legislation including the Cybersecurity and Internet Freedom Act

Select Industry-Specific Laws

Financial Services Companies

Financial services companies must comply with the Gramm-Leach-Bliley Act, which requires them to develop, implement and maintain a comprehensive information security program to protect nonpublic customer information. Financial services companies may also need to comply with standards and regulations issued by regulatory agencies including the following:

- Federal Financial Institutions Examination Council
- Federal Reserve Board
- Federal Deposit Insurance Corporation
- National Credit Union Administration
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- Securities and Exchange Commission
- Financial Industry Regulatory Authority
- Payment Card Industry Security Standards Council

Health and Genetics Related Services Companies

Companies that collect, process, store or transmit health information including genetics related data, are subject to federal and state privacy and data security requirements. The Health Insurance Portability and Affordability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) include detailed rules concerning the privacy and security of personal health information and data breach disclosures. Even industries that are not directly in the health care service industry may have access to personal health information governed by HIPAA and

HITECH. State laws provide civil and criminal sanctions for the disclosure of medical information by types of data or by specific entities holding data and may have broader coverage than federal law.

Europe

In Europe, the EU Data Protection Directive (Directive 95/46/EC) provides that transfers of personal data originating in any one of the 27 member states of the European Union may be made only to member states and to jurisdictions which have been determined by the European Union to have adequate data security standards. The United States is not among those jurisdictions deemed to have adequate data security standards, but Canada is. Because of the strong privacy rights reserved to European citizens under European privacy laws, there may be (at least in some EU countries) a presumption against the legitimacy of cloud computing performed outside of Europe. In part to address this uncertainty, on May 16, 2011, the European Digital Agenda Commissioner opened an online public comment period (Request for Comment) from users and developers of cloud computing to secure their input regarding cross border data protection and liability, standards and operability, and ways to promote research and innovation. The Commission's findings are expected to be released in 2012.

Canada

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) (1990) applies to all private-sector entities that collect personal information on Canadians and personal information used in connection with any commercial activity. PIPEDA requires that individuals consent prior to the collection, use or disclosure of their personal data. It also authorizes the Privacy Commissioner of Canada to investigate citizen complaints and to conduct audits. There is Canadian concern regarding using cloud computing services hosted in the US because Canadian data stored or processed in the US becomes subject to the USA PATRIOT Act.

India

On April 11, 2011, the Government of India implemented new Privacy Rules ("Indian Privacy Rules") under its Information Technology Act ("ITA"). Similar to the United States' Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act, which protect financial and health data, the Indian Privacy Rules require companies that access, possess, or handle "sensitive data or personal information" to adopt "reasonable security practices and procedures." On August 24, 2011, the Indian government issued a press release (Press Note) to clarify that the more onerous portions of the Indian Privacy Rules (Rule 5 regarding securing consent from data subjects prior to collection, and Rule 6 regarding securing consent prior disclosure to third parties) apply only to Indian companies providing services directly to individuals but not to corporate customers.

If you have questions regarding this Bulletin, please contact the authors **Dov H. Scherzer**, co-chair of the firm's Global Outsourcing and Procurement Group at 212.554.7833/ dscherzer@mosessinger.com or **Walter Delacruz**, member of the Privacy and Cybersecurity Group at 212.554.7668/wdelacruz@mosessinger.com.

MOSES & SINGER LLP

Since 1919, Moses & Singer has provided legal services to diverse businesses and to prominent individuals and their families. Among the firm's broad array of U.S. and international clients are leaders in banking and finance, entertainment, media, real estate, healthcare, advertising, and the hotel and hospitality industries. We provide cost-effective and result-focused legal services in the following primary areas:

- Accounting Law Practice
- Advertising
- Asset Protection
- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate/M&A
- Employment and Labor
- Global Outsourcing and Procurement
- Healthcare
- Hotel and Hospitality
- Income Tax
- Intellectual Property
- International Trade
- Internet/Technology
- Legal Ethics & Law Firm Practice
- Litigation
- Matrimonial and Family Law
- Privacy and Cybersecurity
- Private Funds
- Promotions
- Real Estate
- Securities and Capital Markets
- Securities Litigation
- Sports & Entertainment
- Trusts and Estates
- White Collar Criminal Defense and Government Investigations

The Chrysler Building
405 Lexington Avenue
New York, NY 10174-1299
Tel: 212.554.7800 Fax: 212.554.7700

2200 Fletcher Avenue
Fort Lee, NJ 07024
Tel: 201.363.1210 Fax: 201.363.9210
Abraham Y. Skoff, Esq.
Managing Attorney for New Jersey

Moses & Singer LLP is the New York City law firm member of the MSI Global Alliance (MSI). MSI is one of the world's leading international alliances of independent legal and accounting firms, with over 250 member firms in 100 countries - www.msiglobal.org.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.