SCOTT TECHNOLOGY ATTORNEYS

A LEGAL GUIDE TO CLOUD COMPUTING

By Robert J. Scott and Andrew Martin

INTRODUCTION

Many companies are considering implementation of cloud computing services to decrease IT costs while providing the flexibility to scale usage on-demand. The cloud model transfers computing resources from an internally-managed software and hardware infrastructure to a third-party-managed, networked solution. Economies of scale are introduced when the cloud computing vendor offers the same platform to multiple customers, allowing all customers to share the cost burden to manage what is essentially a single implementation provisioned among many corporate users.

Even though cloud computing promises huge cost savings, the risks associated with cloud computing are significant. One of the main characteristics of a cloud-based service is that customer data is being stored and processed by the vendor. This basic design feature creates business risks, regulatory responsibilities, and legal risks which need to be identified and addressed by both the customer and the vendor. Each party must completely understand these risks in order to have a successful cloud computing deal. This document outlines the risks facing a customer contemplating a move to cloud computing and includes sample contractual provisions that show how to address and mitigate those risks.

CLOUD COMPUTING MODELS

Before we address the risks, it is important to understand that not all cloud computing deployments look the same. Cloud computing systems can take different forms. The classic definition (if "classic" is an appropriate term to describe any emergent technology), is the "public" or "pure" cloud where the end-user accesses the software over the public Internet Data and software is stored remotely, on vendor-controlled servers. An alternative model is the "private" cloud where the "cloud" software and data are configured for use by a single organization. A private cloud is cloud computing in the sense that the application is delivered to end-users over a network, but the data remains internally managed, providing companies more control over security and privacy. Most companies will implement a "hybrid" solution which falls somewhere between these two models, where internal and external computing services work in tandem and share information. Depending on which model is contemplated, certain risks may take on increased or decreased significance. But no matter which deployment method is chosen, all risks should be identified and addressed before entering into any cloud computing agreement.

RISKS

BUSINESS CONTINUITY

The nature of cloud computing introduces business continuity risks that are different than any other software agreement a business is likely to consider. Both parties negotiating a cloud computing contract must understand the business continuity risks relating to data (ownership, storage and access), service levels (rights and responsibilities, metrics, subcontractor liabilities and remedies and action plans) and termination (transmission of data and format issues). Each risk should each be specifically addressed in the negotiation and represented in the contract.

DATA LOSS

Because business data is stored and maintained by the cloud vendor, data security issues are at the top of the list of concerns for decision makers. While each party generally endeavors to place all data security risk on the other, neither solution is workable. Ideally, data security risk should be shared between the parties. While there are a number of ways to accomplish this, in our experience the best method is to put data security liability on the vendor, then limit recovery for security breaches to the vendor's insurance limits. This way, each party can identify the amount of risk they are comfortable with, represented by the dollar amount of the insurance limits. An example of an insurance provision mitigating data security and related risks is as follows:

Sample Provision: *Vendor agrees that during the term of this agreement it shall maintain professional liability and errors and omissions insurance including copyright infringement coverage, media liability coverage, and network security and data privacy coverage with minimum aggregate policy limits of not less than two-million dollars. Vendor shall provide Customer a certificate of insurance. In the event of a coverage dispute, Vendor agrees to use all commercially reasonable efforts, including but not limited to filing a declaratory judgment action, to obtain the maximum coverage available.*

SERVICE INTERRUPTION

The next issue that is top-of-mind for decision makers contemplating a move to cloud-based computing services is the access and availability of the service itself. Each party must agree to specific levels of system availability, which is generally contained in a Service Level Agreement (SLA). Defining service level metrics, remedies and action plans, and subcontractor liability will help to balance the risk of service interruption.

SERVICE LEVEL METRICS

Service levels should be continuously monitored and reported to determine whether the vendor is meeting its availability requirements. To be a meaningful representation of service levels, the metrics used for measurement can be customized to fit the customer's needs. When choosing metrics, consider the following:

1) metrics should provide the vendor with incentive to act in the expected manner;
2) metrics should not be relatively easy to collect; and,
3) metrics should be under the vendor's control.

To determine which metrics represent the best measurement of service levels, each party's IT specialists must participate in this discussion. Metrics the business person considers sufficient and reasonable may not accurately address the availability of the system or may be impracticable to collect.

SUBCONTRACTOR LIABILITY RESPONSIBILITY

Many vendors deliver a cloud solution that relies on third party software. In some cases, the cloud platform may be composed of two or more integrated cloud bundles. Customers should inquire as to the vendor's use of third party services or software and ensure that the SLA addresses subcontractor liability for third party service failures.

Sample Provision: *Vendor acknowledges the use of third party software to deliver the Service and accepts responsibility for service failures attributable to failures by any third party software used by the Service.*

From the vendor's perspective, carving out responsibility for third party software purchased and operated by the client is important. Vendors should limit responsibility for the normal operation of their software to the extent the customer uses approved third party software for access (e.g., define an approved web browser). A good agreement will define the third party software endorsed by the vendor and limit the warranty to those products only:

Sample Provision: *Vendor does not warrant that the Software shall operate in combination with other software selected by Customer other than any Approved Third Party Software as noted.*

REMEDIES AND ACTION PLANS

Because there will be service failures, definitions of remedies and action plans for resolution of service failures are essential components of the SLA. Good SLAs not only define service level failures, but they describe the procedures to be used to resolve the issues. Most SLAs will include a customer credit for downtime that exceeds a specific service level offered by the vendor. Larger credits are given for downtime associated with business-critical processes. In addition, SLAs should include a target timeframe for resolution of any issue, where such targets would change depending on the nature of the service outage. Where an outage lasts for a significant period of time, it is useful to require the vendor to produce an action plan for resolution of the issue:

Sample Provision: *Notwithstanding Vendor's obligation to continue to perform as required under the Agreement and Customer's remedies set forth herein, in the event of a Service Level Failure, Vendor shall upon request from Customer promptly investigate the root causes of such Service Level Failure and shall provide to Customer (within five (5) days after knowledge of such Service Level Failure) an analysis of such root causes and a proposed corrective action plan (the "Corrective Action Plan"). The Corrective Action Plan shall include, at a minimum: (i) a commitment by Vendor to Customer to devote the appropriate time, skilled personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of, the Service Level Failure; (ii) a strategy for developing any programming/software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, the Service Level Failure; and (iii) time frames for implementation of the Corrective Action Plan. There shall be no additional charge (other than those fees set forth in the Agreement) for Vendor's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan*

TERMINATION OF THE AGREEMENT

Every engagement will eventually come to an end. In the case of cloud computing, the end of the agreement can be especially painful for the customer if it does not properly prepare for termination during contract negotiation. Specifically, there must be agreement as to who owns any data upon termination (the customer should, in most cases) and how that data is to be produced. The following provision stops short of defining an actual transmittal

method, but it does provide that the data is owned by the customer and will be delivered to the customer at the termination of the agreement:

Sample Provision: *Regardless of the reason for termination, Vendor will use commercially reasonable efforts to deliver all of Customer's Data to Customer in a mutually agreed upon electronic format with ninety (90) days following the termination of the Agreement.*

LEGAL RISKS

Most business continuity risks inherent to a cloud computing platform are obvious, but the legal risks involved are less apparent. These legal risks include litigation and discovery procedures and intellectual property protection and enforcement.

LITIGATION AND DISCOVERY

Litigation and technology are inexorably linked—discovery of relevant evidence does not occur without resorting to some level of IT systems and controls. Courts are becoming more adept at deciphering the capabilities and limitations of various technologies as they pertain to retaining and producing documents during the discovery phase of litigation. Today, a court will likely not accept a litigant's explanation that their data was stored and managed "somewhere else." Any data stored in the cloud must be accessible by the customer in the event of litigation.

All cloud computing agreements where the customer is potentially storing data which may someday be relevant to a legal dispute should define methods and policies for data retention and discovery production that provide significant control to the customer. In addition, customers should be able to match the data retention policies in the cloud service to those which they implement internally. The following provision requires the vendor to comply with litigation hold requests from the customer and matches the data retention procedures of the service offering to the customer's internal data retention policy:

Sample Provision: *Vendor acknowledges that Customer Data stored on the Vendor's servers may, from time to time, be pertinent to a litigation matter in which Customer is involved. Upon notice from Customer, Vendor will take commercially reasonable steps to initiate the requirements outlined in the Customer Litigation Hold Notice document (Exhibit A). Furthermore, all Customer Data will be subject to the data retention policies outlined in Customer Data Retention Policy (Exhibit B) and Vendor warrants that the technology employed by Vendor is sufficient to meet these requirements.*

INTELLECTUAL PROPERTY OWNERSHIP

In most cases, the data provided by the customer is owned by the customer. Customers must ensure the contract explicitly defines customer data and ownership. In some instances it is not readily apparent who retains ownership over the content.

For instance, it is common for a vendor to customize its service offering to meet a customer requirement. In this circumstance, both parties must take care to establish customization ownership. The additional code written for the customization could be considered the property of the vendor or a "work for hire" owned by the customer. Where it is agreed that the vendor owns the code, the customer may wish to retain exclusivity over the customizations for the duration of the agreement. Upon termination of the agreement, the code may be retained by the vendor and provided to other customers. The provision below separates functional customizations from design content, provides exclusivity to all customizations to the customer for the duration of the agreement:

Sample Provision: *If, and only to the extent expressly stated below that Vendor shall provide a Unique Design Component, then Customer will have exclusivity with respect to that Unique Design Component for the duration of the Agreement. Exclusivity means that Vendor will not utilize the same or substantially similar Unique Design Components for another customer during the term of the Agreement. Unique Design Components shall be owned by Customer as works made for hire in accordance with the terms hereof.*

REGULATORY ISSUES

Compliance with industry and regulatory requirements is perhaps the most vexing issue facing a customer contemplating a move to the cloud. From HIPAA to FTC Red Flags Rules to state security and privacy statutes, more companies are required to comply with one (or sometimes many), data privacy and security regulations.

INDUSTRY REGULATION

Depending on the customer's industry, compliance with data privacy and security regulations may be required. In many cases, cloud vendors selling their product to customers in industries subject to data security regulations are considered "covered entities" that are subject to those regulatory requirements. Examples of federal and state data security and privacy regulations and industry compliance include:

- **FTC Red Flags Rule** – requires financial institutions and creditors to, among other things, monitor and prevent identity theft.
- **HIPAA & HITECH** – establishes security requirements and controls for entities that handle protected health information. HITECH will formally extend those requirements to 3rd party service providers.
- **Gramm-Leach-Bliley Act** – requires financial institutions to develop and implement a written information security plan.
- **Payment Card Industry Data Security Standard (PCI)** – applies to all organizations that hold, process or exchange cardholder information.
- **Massachusetts Data Privacy Law** – defines security procedures to safeguard data where personal information about a resident of Massachusetts is stored.

Whether and to what extent a vendor or customer is a covered entity under privacy and data security regulation is something both parties must carefully evaluate during negotiations. Where a specific regulation is particularly important to the customer or vendor, language in the contract should closely track the applicable language of the regulation. In instances where regulatory compliance is of marginal concern, a general compliance term as follows may be sufficient:

Sample Provision: *Vendor shall be responsible for maintaining compliance with applicable Laws and Regulations related to its Software, Servers, and Hosting services and shall indemnify Licensee and its officers, directors, employees, and representatives against, and hold them harmless from: (1) any claims or allegations made or that arise from or relate to any such obligations (2) any litigation, arbitration, judgments, awards, settlements, damages, expenses, losses, attorneys' fees, and costs arising from or relating to any such claims or allegations. Vendor may, at any time, change its procedures to remain compliant with the Rules and Regulations.*

In any case, consultation with an attorney experienced in the regulations and requirements for a specific industry is recommended before entering into any cloud computing contract.

CONCLUSION

The most important step to take before entering into any cloud computing agreement is to identify the applicable risks described above to determine your company's comfort level with respect to each. Begin the discussion of risk balancing issues early in the negotiation. Lengthy, unsuccessful negotiations can be avoided if each side is clear as to their "deal-breakers" with respect to these risks. When the discussion is focused solely on cost and technical capabilities of the cloud service, risk-sharing conversations can come too late in the process and derail the entire deal. Before signing a cloud computing software contract, it is important to consult with an attorney experienced with identifying risks associated with cloud agreements who can carefully construct the agreement to balance risks in the manner most appropriate for your situation.

About the author Rob Scott:

As the managing partner of Scott & Scott, LLP, Robert has built a global practice representing clients on issues where technology, media and the law intersect. A boutique firm with international reach, Robert ensures that Scott & Scott is committed to legal excellence, unparalleled customer service, and cost-effective strategies that deliver positive results. Representative clients range from multinational corporations to local mid-market businesses spanning all industries.

Get in touch: rjscott@scottandscottllp.com | 800.596.6176

About the author Andrew Martin:

As an associate attorney with extensive prior experience advising information technology start-ups, Andrew's practice focuses on finding solutions for his clients' intellectual property issues. Due to his extensive experience in the software and technology industries, Andrew understands both the practical and legal issues involved in IP licensing agreements and disputes. In addition to licensing, Andrew helps his clients find new ways to use existing technologies to assist his clients in areas such as data privacy compliance. Andrew uses his diverse background which includes founding a record label and working for a world-wide concert promoter when counseling the firm's entertainment clients.
Get in touch: amartin@scottandscottllp.com | 800.596.6176