Cloud Service Agreements: Avoiding the Pitfalls of the Cloud as a Commodity

Amy Mushahwar, Esq.

ReedSmith

The business of relationships.

What's New? Not That Much….

- Some have their heads in the cloud… we prefer to stay down in the weeds and know the details.
- Cloud Computing holds all of the risks of a typical web hosting shared services arrangement.
- The key is planning ahead and avoiding take-it-or-leave-it agreements with standard, non-negotiable terms.
- If the cloud computing service provider is not willing to negotiate a contract, then the provider may not be worth the supposed cost savings.

ReedSmith

The business of relationships.

Oy Veh! Where do I begin?

- Due Diligence
  - Data Security
  - Performance
  - Terms of Service, Warranty and Indemnification
  - Data Segregation
  - Governmental and Third-Party Litigation Access
  - Trade Secrets and Confidential Information
  - Exit Plan

ReedSmith

The business of relationships.

The Privacy/Data Security Analysis Alone Demands Caution…

- **Federal**: Multiple sector-specific privacy laws:
  - Education information – FERPA
  - Medical information – HIPAA, the HITECH Act
  - Financial data – Gramm-Leach-Bliley ("GLBA")
  - Disclosure to law enforcement agencies – USA Patriot Act
  - Electronic communications – ECPA
  - E-Discovery – Federal Rules of Civil Procedure ("FRCP")
- **State**: Data-breach statutes, SSN laws, health privacy, financial privacy and the like.
- **International**: Personal data within EU – The European Union Data Protection Directive; Data laws of non EU-States (i.e. Australia, Canada and now, Mexico)
- **Contract**: Payment Card Industry Standards and any other contractual privacy provisions.

ReedSmith

The business of relationships.

Data Security:
Much More than SAS 70 Certification

- Data Flows
- SAS 70 Certification
- Requirements for Physical and Logical Security
- Single Point or Multipoint Server Models
- Privacy Policy Review
- Data Migration (in and out of system)
- Data Backups & Recovery
- Audits? (PCI Compliance/Safe Harbor)

ReedSmith

The business of relationships.

Performance / SLAs

- 24/7/365 uptime of cloud services is of critical importance. The inability to access data stored in the clouds can cause significant business interruption and lost revenue.
  - Discuss Power
  - Multiple Communications Links?
  - Recent Service Level Payments? Recent Outages?
  - Maintenance Windows and Access During Planned Outages?
  - Data Restoration Timing?

ReedSmith

The business of relationships.

Terms of Service, Warranty and Indemnification

- Vendors tend to provide vague terms of service, warranty nothing and make no indemnification promises. The worst clauses that I have seen are below:
  - The unilateral right to limit, suspend, or terminate the service (with or without notice) (and for any reason)
  - Disclaimer of liability relating to service quality and availability (instead, there should be clear initiation and ongoing service levels)
  - Uptime and reliability percentage promises (where the vendor discerns the end points of uptime measurements)

Terms of Service, Warranty and Indemnification (continued)

- Disclaimer of all warranties, including the implied warranties of merchantability and of fitness for a particular purpose
- Disclaimer of liability for third-party action
- Remedy limitations, including total damages capped (such as a return of fees paid), and/or exclusion of consequential damages (such as loss of profits/revenue)
- Indemnification: does it look like a “get-out-of-court/damages-free card”? Has the provider so narrowly tailored the section to indemnify it against actions that are in fact not its responsibility

Data Segregation

- Currently, most cloud service providers offer their services on a shared server basis. Special care should be taken to ensure that your company's data is not inadvertently mingled with that of any other customer (especially, a competitor). The following questions should be asked to ascertain the provider's data segregation procedures:
  - Ensure that no one other than your company has access to the data, even if the customer is hosted on a shared server?
  - How frequently does the provider monitor its server to confirm that data is properly segregated?

Governmental and Third-Party Litigation Access

- Cloud Computing and the right to governmental access is an issue before the Supreme Court in Ontario v. Quon. Given the present ambiguity in the state of the law, the outsourcing agreement should contemplate the following:
- For instance:
  - Is the provider required to notify the user if the provider receives a subpoena, search warrant, or other lawful request for user information? (Note, that there are some subpoenas, where the government forbids customer notification).
  - Will the cloud provider seek a protective order to prevent and/or limit disclosure of company data?
  - In the event of litigation, how are litigation holds enforced? What are the procedures to make sure user data is segregated and retained?
  - How are e-discovery requests handled? How would metadata be protected? And how is information searched for and retrieved?
  - Which party bears the costs associated with processing data for discovery purposes?

Trade Secrets and Confidential Information

- Even with good contractual provisions storage of a company's trade secrets with a cloud provider carries significant risk.
- Under the Uniform Trade Secrets Act, for a company's proprietary information to be accorded trade secret status, the trade secret must be, at a minimum, the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
- Whether a transfer of trade secrets to a cloud provider extinguishes the trade secret has yet to be ruled upon. A company's trade secrets may lose their status as such even in circumstances where the cloud provider commits to keeping confidential any information it receives.
- Certainly, where the cloud provider's terms of service allows the provider to see, use, or disclose information, this may degrade the user's claim that the information is a trade secret.

Exit Plan

- An exit plan defining each party's obligations in the event of a termination of services should also be clearly set forth in the agreement, consider the following:
  - Reasons for Termination
  - Timing for Termination (allowing for a transition plan?)
  - Risk of Provider Lock-in
  - Data Return / Data Backup
  - Transition Assistance / Data Format / Data Transfer
  - Data Disposal
  - Encryption Complications

A Few Words from Our Tax Lawyers…

Cloud computing, including cloud services, is one of the most notable, recent targets in the federal and state governments' search for revenue. Federal legislation was introduced in July 2010 that would impose sales tax on digital commerce, including possibly some cloud services, and many states have begun to expand their state tax laws to reach cloud products and services.

The primary tax issues involved in cloud computing and cloud services are:

- Nexus – Contacts with the Jurisdiction (*e.g.*, income, gross receipts, sales and use)?
- Taxability – Service Characterization Dictates Treatment (*e.g.* a good, service, data processing, infrastructure, platform, and software services).
- Sourcing – revenue sourced to destination, origination, ugh!

Encryption: Avoiding Information Transfers vis-à-vis Encryption

- Emerging view regarding encryption is if the service provider does not have the encryption key, then information has technically not been transferred
  - If data is encrypted in the cloud, the service provider has not been given access to the data.
- However, a company may have reasons to provide the service provider with an encryption key. What if the key is lost or there is employee turnover?
  - An encryption key may be held in trust by a third-party so that the key is not held by the service provider.
  - A key held in trust is then kept safe and available if needed later

Attorney- Client Privilege Expectations When Transferring to the Cloud

- Normally, when one transfers information to a third-party, confidentiality and attorney-client privilege is moot.
  - There can be no expectation of privacy when information has been transferred to a party that has no obligation to keep the information confidential.
- So, is the cloud considered a third-party??
  - Common law view is that the cloud IS a third party and there is no expectation of privacy
  - Emerging modern view taken by some states' ethics panels is that if the service provider does its due diligence and keeps the information confidential and secure, when an attorney puts information in the could, privilege DOES NOT dissolve.

ReedSmith

The business of relationships.

Department of Commerce Information Security Report

- Released yesterday.
- Increases the visibility of cybersecurity and effectuates President Obama's cyber security mandate.
- Expect cybersecurity/cloud security legislative movement in the next year.

ReedSmith

The business of relationships.

Conclusion

- Sometimes the seemingly amazing cost savings of a commodity provider fails to reveal the hidden regulatory costs that could emerge down the line.
- We recommend cautiously exploring each solution with full network documentation, before entering into a cloud outsourcing arrangement.

ReedSmith

The business of relationships.