LEGAL ISSUES IN CLOUD COMPUTING

RITAMBHARA AGRAWAL

INTELLIGERE

2nd IndicThreads.com Conference On Cloud Computing

3,4 JUNE 2011

PUNE, INDIA

CLOUD COMPUTING

Cloud computing is a model for enabling 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 provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software anddata are stored on servers at a remote location.

The key characteristic of cloud computing is that the computing is "in the cloud"; that is, the processing (and the related data) is not in a specified, known or static place(s)

Delivery Models

- Cloud software as a service (SaaS) : Use the provider's applications running on a cloud infrastructure. Software running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.
- Cloud platform as a service (PaaS) : User-created applications running on a cloud infrastructure.
- Cloud Infrastructure as a service (IaaS) :Processing, storage, networks, and other fundamental computing resources running on cloud infrastructure.

Deployment Methods

- **Private cloud (Internal Cloud) :** The cloud infrastructure is operated solely for a single organization.
- **Public Cloud :** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Community Cloud :** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on-premises or off-premises.
- **Hybrid Cloud :** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Cloud Computing: Legal Challenges

- Liability
- Security
- Risk allocation
- Date Retention Issues
- 3rd party contractual limitations
- Regulatory compliances
- Control over physical location of the data
- Security breach
- Trade secret protection
- Hacking of cloud provider
- Financial liability of cloud vendor
- Legal/practical liability for force majeure events
- IPR issues
- Jurisdiction and court of law

Cross Border Legal Issues

- Cloud Cloud inherently being stateless and serves located in different locations and countries creates issues related to conflict of laws, applicable law and jurisdiction.
- Cross-border data flow, potentially conflicting regulations, applicable regulations

Involvement of multiple parties

- Cloud services usually involve multiple parties which makes onus and liability shift on one another. Liability and responsibility of sub-contractors is often limited or disclaimed in entirety.
- Contractual privity lacks between the parties which makes it difficult for the client to bind a provider for a breach.
- Agreements should include liability of provider for acts of sub-contractor.
- Right to conduct due diligence and to understand the model of delivery of services should be given to the customer.

Privacy and Security

- Multi-tenant architecture
- Data from different user are usually stored on a single virtual server
- Multiple virtual servers run on a single physical server
- Data security depends upon the integrity of the virtualization

Service Level Agreements

- Cloud services are usually provided on standard service level agreements which are usually non-negotiable.
- Even if negotiation is not agreeable for SLA, higher degree of reporting should be integrated in the agreement.
- Additional options for termination should be provided.

Issues with Service Level Agreements

- Standard mass market contracting terms are used
- Non-negotiable (often click through)
- Little opportunity to conduct due diligence
- Strong limits on liability (including direct liability)
- Terms often subject to change without little notice
- Risk is generally shifted to user through provider friendly agreements

Audit Trail

- As data is on continuous move and flow in the cloud services, client should have the right to know where and by whom its data is stored, accessed, transferred and altered.
- Confirm whether the vendor provides the audit trails rights or not.

IPR and Ownership Issues

- Trade Secret Protection. As third parties might have access to data, which can be detrimental to trade secrets of a company.
- Companies should have non-disclosure agreements with the vendor.
- Ensure that no rights in IPR are transferred to the vendor.

Exit Issues

- In case a user has to change provider in the future the options for portability and interoperability are critical issues to be considered.
- In case of exit can the records be successfully accessed?
- Can data be extracted from the cloud?
- Obligations of each party in case of exit.

Hacking of cloud vendor

- In the event that cloud vendor system is hacked, does the owner of the data has the right to move against the vendor for claiming lost profits.

Legal and practical liability for force majeure events

- What happens to the owner's data in case of a disaster? How much is the vendor liable for the recovery and restoration of the data?
- What are the back-up mechanisms for recovery of the data?

Jurisdictional Issues

- In cloud services location of data is usually uncertain. The owner of data is not aware of the country where the data is stored. The physical location of the data raises the question of law to be governed and jurisdiction. Its important to be aware of the prevailing law in that particular nation.
- What if a dispute arises, what will be the place of jurisdiction. The owner of the data should be aware of the country's court system which will govern the conflict arose between the parties.
- For eg. The owner is based at India and cloud service provider is based in the US. The vendor would prefer jurisdiction of American Court. But can the owner afford to contest the matter in American court.

Risk allocation/mitigation/insurance

- No vendor offers a 100% guarantee. The most trusted vendor can also fail.
- Replication of data should be done and application should be available at multiple sites.

Recommendations

- Customers and cloud providers must have a mutual understanding of each other's roles and responsibilities related to electronic discovery, including such activities as litigation
- Cloud providers are advised to assure their information security systems are responsive to customer requirements to preserve data as authentic and reliable, including both primary and secondary information such as metadata and log files.
- Data in the custody of cloud service providers must receive equivalent guardianship as in the hands of their original owner or custodian.
- Plan for both expected and unexpected termination of the relationship in the contract negotiations, and for an orderly return or secure disposal of assets.
- Pre-contract due diligence, contract term negotiation, post-contract monitoring, and contract termination, and the transition of data custodianship are components of the duty of care required of a cloud services client.

Recommendations

- Knowing where the cloud service provider will host the data is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data.
- As the custodian of the personal data of its employees or clients, and of the company's other intellectual property assets, a company that uses Cloud Computing services should ensure that it retains ownership of its data in its original and authenticable format.
- Numerous security issues, such as suspected data breaches, must be addressed in specific provisions of the service agreement that clarify the respective commitments of the cloud service provider and the client.
- The cloud services agreement must allow the cloud services client or designated third party to monitor the service provider's performance and test for vulnerabilities in the system.
- The parties to a cloud services agreement should ensure that the agreement anticipates problems relating to recovery of the client's data after their contractual relationship terminates.

Recommendations

- Involve Legal and Contracts Teams. The cloud provider's standard terms of service may not address your compliance needs; therefore it is beneficial to have both legal and contracts personnel involved early to ensure that cloud services contract provisions are adequate for compliance and audit obligations.
- Right to Audit Clause. Customers will often need the ability to audit the cloud provider, given the dynamic natures of both the cloud and the regulatory environment.
- A right to audit contract clause should be obtained whenever possible, particularly when using the cloud provider for a service for which the customer has regulatory compliance responsibilities.