

Legal Issues Associated with Cloud Computing

Laurin H. Mills

May 13, 2009



What Is Cloud Computing?



- The “cloud” is a metaphor for the Internet
 - Leverages the connectivity of the Internet to optimize the utility of computing
- It is not new!
 - Search is a cloud application
 - Gmail, other Internet-based email services are cloud applications
 - Social networking sites are cloud applications
 - Similar to time-sharing and service bureau services from the mainframe days, or ASP’s from the 90’s
- Accessible anywhere with Internet access
 - There are public, private, managed and hybrid clouds

Cloud Computing Delivery Models

- IT infrastructure – hardware, storage, network – sold as a service (IaaS)
- Application development platform sold as a service (PaaS)
 - Tools to develop applications in a standard environment
 - New businesses and applications can be developed faster and with much less investment/risk than before
 - Easier and faster to scale
- Software as a Service (SaaS)
 - User-facing software applications

The Most Basic Issues

- What should live in the cloud?
 - There are unavoidable risks associated with having mission critical systems and sensitive company or customer data residing in the “cloud”
 - To be successful, cloud vendors will develop ways to minimize these risks, but they will never go away
- Data, application and network back-up and redundancy will be essential; so will insurance
- Open standards and use of open source software will be critical to the growth of this concept
- Privacy/data security
- Complying with a patchwork of federal and state privacy laws

Be Prepared for Change

- Cloud industry is immature and growing rapidly
- New players will rapidly emerge to fill new market niches
- Consolidation of the industry at some point is inevitable
 - You may not be as comfortable with new entity
 - Google, Amazon, IBM, Microsoft all active in this area
 - Big players will create standards for security and governance
- Cloud computing is disruptive to existing business models and IT practices
 - Disruptive technologies attract players who may not be around for the long term

Types of Issues

- Location (where is your data; what law governs?)
- Operational (including service levels and security)
- Legislation/Regulatory (including privacy)
- Third-party contractual limitations on use of cloud
- Security
- Investigative/Litigation (ediscovery)
- Risk allocation/risk mitigation/insurance



Location Issues

- Where will your data be located?
 - The cloud may be the ultimate form of globalization
- What law governs?
 - You may or may not be able to control this by contract as the law in some countries can trump contractual provisions
 - State law is becoming increasingly relevant
- Storing data in certain regions may not be acceptable to your customers, especially the government



Operational Issues



- Vendor lock-in issues
 - Will you be bound to a certain application; platform; operating system?
 - Some critics, such as Richard Stallman, have called it “a trap aimed at forcing more people to buy into locked, proprietary systems that will cost them more and more over time”
- Can you transfer data and applications to and from the cloud?

Operational Issues cont'd



- Backup/data restoration
- Disaster recovery
- Acceptable service levels
- What do you do if the Internet crashes?
 - How is that risk allocated by contract?
- Data retention issues
 - There many legal and tax reasons that company must retain data longer than cloud vendor is prepared to do so

Regulatory/Governance Issues

- The more of these issues you have, the slower you will move to cloud computing
 - Early growth in cloud computing will come from small and medium sized businesses and give them a competitive advantage
 - Portion of cost savings will have to be reinvested into increased scrutiny of security capabilities of cloud providers
- Some regions, such as the EU, have stringent rules concerning moving certain types of data across borders
- Cloud computing not regulated – yet

Regulatory/Governance Issues cont'd

- Patriot Act/UK Regulation of Investigatory Powers Act
- Stored Communications Act (part of ECPA)
- National Security Letters (may not even know of investigation)
- HIPPA (health-related information)
- GLB (financial services industry)
- FTC and state privacy laws
- ITARS, EARS, other export or trade restrictions will impact where data can be stored and who can store it

Regulatory/Governance Issues cont'd

- Video rental records
- Fair Credit Reporting Act
- Violence Against Women Act
- Cable company customer records
- Privacy Act (for federal agencies)



Contracts Will Be The Key Legal Enforcement Mechanism

- Privileged user access
 - Who has access to data and their backgrounds
- Regulatory compliance
 - Vendor must be willing to undergo audits and security certifications
- Data location
 - Can you control the physical location of your data?
- Security
 - Implementation is a technical matter; responsibility is a legal one

Key Contractual Issues cont'd

- Data segregation
 - Use of encryption to protect data – a sometimes tricky issue
- Recovery
 - What happens to your data and apps in the event of a disaster?
 - You should have test procedures in place
- Long-term viability
 - What happens to data and apps if company goes out of business?
- Investigative support
 - Will vendor investigate illegal or inappropriate activity?
- What happens in the event of a security breach?

Security Issues

- Physical security
 - Physical location of data centers; protection of data centers against disaster and intrusion
- Operational security
 - Who has access to facilities/applications/data?
 - Will you get a “private cloud” or a service delivered more on a “utility” model?
- Programmatic security
 - Software controls that limit vendor and other access to data and applications (firewalls; encryption; access and rights management)
 - Encryption accidents can make data unusable

Investigative/Litigation Issues

- Third party access
 - Subpoenas
 - You may not even know about them if vendor gets the subpoena
 - Criminal/national security investigations
 - Search warrants; possible seizures
- EDiscovery
 - How are document holds enforced; metadata protected; information searched for and retrieved?
- You must have clear understanding of what cloud provider will do in response to legal requests for information

Intellectual Property Issues

- The big issue is trade secret protection
 - If third parties have access to trade secret information, that could destroy the legal protection of trade secrets
 - This can be ameliorated by appropriate contractual non-disclosure provisions
- Same concern for attorney-client privileged information



Risk Allocation/Management

- No benchmarks today for service levels
- No cloud vendor can offer a 100% guarantee
 - The most trusted and reliable vendor can still fail
 - Should replicate data and application availability at multiple sites
 - Should you escrow data or application code?
- A premium will be charged based on the degree of accountability demanded
- Responsibility of customer to determine if it is comfortable with risk of putting service in the cloud

Insurance



- Will business interruption insurance provide coverage if your business goes down because of problem at cloud vendor?
- Do CGL or other types of liability coverage handle claims that arise from privacy breaches or other events at the cloud level?
- Are you covered if your cloud vendor gets hacked?

Checklist of Things to Consider

- Financial viability of cloud provider
- Understand cloud provider's information security management systems
- Plan for bankruptcy or unexpected termination of the relationship and orderly return of disposal of data/applications
 - Vendor will want right to dispose of your data if you don't pay
- Contract should include agreement as to desired service level and ability to monitor it
- Negotiate restrictions on secondary uses of data and who at the vendor has access to sensitive data

Checklist Cont'd

- Negotiate roles for response to Ediscovery requests
- Ensure that you have ability to audit on demand and regulatory and business needs require
 - Companies subject to information security standards such as ISO 27001, must pass to subs same obligation
- Make sure that cloud provider policies and processes for data retention and destruction are acceptable
- Provide for regular backup and recovery tests
- Consider data portability application lock-in concerns
- Understand roles and notification responsibilities in event of a breach

Checklist cont'd

- Data encryption is very good for security, but potentially risky; make sure you understand it
 - Will you still be able to de-encrypt data years later?
- Understand and negotiate where your data will be stored, what law controls and possible restrictions on cross-border transfers
- Third-party access issues
- Consider legal and practical liability for force majeure events
 - Must be part of disaster recovery and business continuity plan
- There is no substitute for careful due diligence

NIXON PEABODY_{LLP}
ATTORNEYS AT LAW