BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

Legal Issues in the Cloud: A Case Study

Jason Epstein

Outline

- Overview of Cloud Computing
  - *Service Models (SaaS, PaaS, IaaS)*
  - *Deployment Models (Private, Community, Public, Hybrid)*
  - *Adoption*
- Different types of organizations using the “Cloud”
- In general: Service Model, Deployment Model, vendor and type of organization all impact negotiation and legal issues
- Case Study: Health care buying direct using public cloud

Source: www.nist.gov

Service Models

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). ***The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.***
- ***Example:*** **Salesforce.com, Google docs, Yahoo! mail.**

Source: www.nist.gov

Service Models (cont'd)

- *Cloud Platform as a Service (PaaS)*. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. ***The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.***
- ***Example:*** PaaS is a development platform for developers. Salesforce.com's "Force.com"; Windows Azure Platform.

Source: www.nist.gov

Service Models (cont'd)

- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. ***The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).***
- ***Example:*** Fully outsourced managed hosting and development environments. Google, IBM, Amazon.com etc.

Source: www.nist.gov

Deployment Models

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Source: www.nist.gov

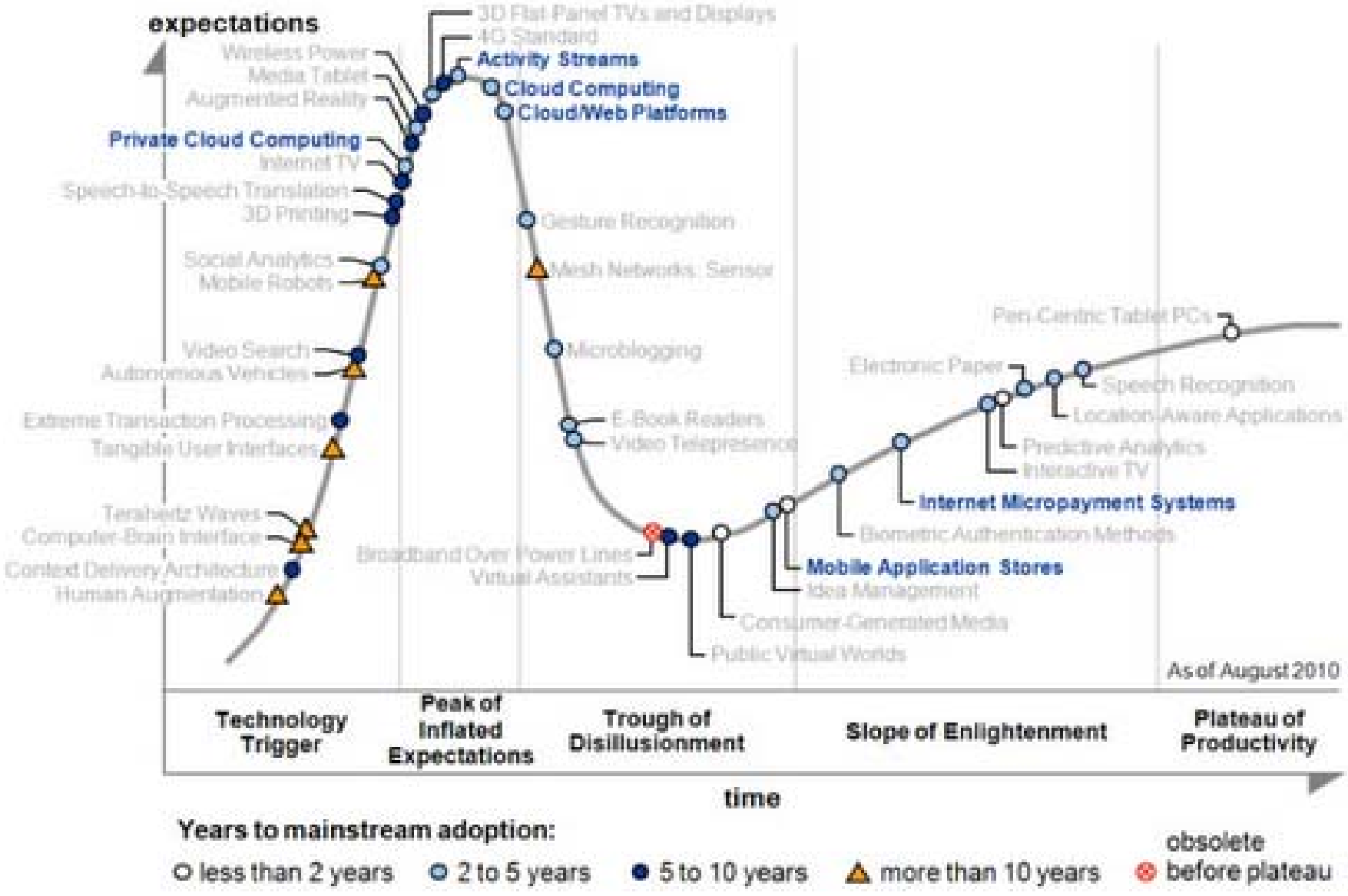
Deployment Models (cont'd)

- *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.
- *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 (e.g., cloud bursting for load-balancing between clouds).

Source: www.nist.gov

Cloud and Platforms

Source: Gartner



Cisco Systems, Inc. has identified four types of organizations:

- Small and medium-sized businesses (using the public cloud)
- Large enterprises (private and hybrid cloud models more common but still use public cloud)
- Public-sector organizations
- Service providers

Source: Cisco Systems, Inc.

In addition, regulated entities deserve a special category such as in the health care or financial spaces

- Regulated industries have additional focus on applicable regulation, especially for privacy and security

Source: Cisco Systems, Inc.

Case Study

- Use of public cloud for e-mail, collaboration applications, documentation generation, and data storage and processing by a health care entity. HIPAA/HITECH Act applicable.
- Mostly buyer's perspective.
- Cost driven: OpX vs. CapX
- Direct to the vendor and not through reseller.
- Other challenges: service offerings and vendor agreements change during negotiations.
- And here are (some of) the business/legal issues . . .

Understand the Business Model

- Understand that the business is still developing and changing over time.
- Understand the service offerings and options, especially relating to privacy, security and eDiscovery.
- Understand what is not included.

Understand the Vendors

- The culture of the vendors drives attitudes towards legal agreements.
- Culture of consumer vs. business (enterprise) deals.
- What is the culture regarding negotiation?
  - When do you get past the salesforce
  - What is the escalation procedure
- Use of subcontractors?

Understand the Contract

- Many public cloud providers use multiple levels of contracts.
- Those contracts often link to other documents such as privacy policies, acceptable use policies, security policies, service level agreements, technical support obligations, and others that should, if done correctly, become part of the overall contract.

Pick Your Team

- Due to the nature of cloud computing, at least for now, most major cloud initiatives require the expertise of more than one lawyer or contract negotiator.
- In this case, the negotiating team is:
  - the business technology lawyer
  - a privacy lawyer;
  - a security lawyer; and
  - an e-discovery lawyer.
- Some of the above is for due diligence purposes.

Pick Your Team (cont'd)

- During negotiation, it is often beneficial to have an all-hands meeting between the vendors (SMEs), the sales representative, contract negotiator and/or lawyers as well as the legal team representing the buyer.

Service Descriptions

- Different companies view service descriptions differently.
- Some vendors do not have service descriptions per se but include some sort of documentation online that is incorporated into the agreement.
- Other vendors try to avoid including service descriptions in the contract.

Business Associate Agreement

- Most vendors will generally agree to some sort of business associate agreement.
- Some vendors still fight taking on that obligation.
- The Office of Civil Rights (OCR) has jurisdiction (among others).
- What is a “business associate?”

Security

- A “covered entity” must prove it is HIPAA security compliant (including through its vendors).
- Compliance obligations flow back to the covered entity, so due diligence on the vendor as well as contractual assurances are necessary.
- This includes the requirement to remain in compliance as the law changes or allow remedies to exist in the contract.
- Most vendors have security language to review, if asked.
- Audits and SAS 70 Type II, ISO 27001.

Data Breach

- Most vendors will recognize that they need to comply with security breach laws.
- Due diligence on the vendor is key in this area as well as having sufficient contractual language for all parties to be able to comply with data breach rules.
- Remedy?

E-discovery

- Due diligence should be required on capabilities of the vendor and related e-discovery tools and service descriptions/contractual language.
- Where/how is the data stored?
- How will the tools work for compliance, will they be for e-mails only or for other information stored in the cloud (such as instant messaging or documents)?
- What is the response plan for responding to third-party subpoenas or other attestation requests and witness availability?
- Right to Conduct Forensics?

E-discovery (cont'd)

- Dealing with privacy of individual's use and social network policies.
- Cross-border discovery issues (conflict between U.S. discovery rules and foreign privacy laws and blocking statutes potentially preventing disclosure).
- Litigation holds/Retention Policies.
- Metadata.
- Location of documents may make access to them by government/third parties accessible other than going through client directly.
- Expectation of Privacy and Attorney-Client Privilege (and company policies!).
- How is data actually "destroyed?" Rewritten?

Service Level Agreements

- Most SLAs relate to “up time” although there are some virus and security SLAs.
- Sole and exclusive remedies clauses.
- Warranty language regarding SLAs.
- Uptime/Schedule or Authorized Downtime/Response Time/Permitted outages.
- Uptime SLAs vs. Functionality SLAs

Modifications to the Service

- Most vendors start with proposition that they can modify service at any time.
- Especially in a regulated environment, due diligence is performed on the service to determine capability and that service is relied upon.

Modifications to Terms and Conditions

- Most agreements retain the ability to change the terms and conditions of the underlying agreement, including those incorporated by reference, at any time.
- This can be troubling because it would apply to privacy and security policies as well, in addition to e-discovery.

Suspension of the Services

- Distinction of suspension of an end-user account versus the services as a whole.
- Business continuity.
- Compliance with health care and other obligations.

Termination and Assistance Services

- Most vendors do not have explicit terms for termination assistance other than providing the ability to download data for a certain period of time.
- It may not be practical to not have access to the service during the termination period. Consider the e-mail system.
- What about security violations, multiple SLA breach, violation of privacy and security policies . . . Not susceptible to “cure.”

Disaster Recovery and Business Continuity

- Due diligence requirements.
- Disaster recovery versus SLAs for up time.
- HIPAA: 45 CFR § 164.308(a)(7)(ii).

Privacy Policies

- Cloud vendors have links to numerous privacy policies incorporated into the agreement.
- Applying these privacy policies to the business versus individual users who sign up for a free service period.
- Modifications of privacy policies.

Data Transfer/Offshoring

- Understanding the practice of the current vendor.
- Capabilities differ based on deployment model as well.

Warranty

- Services in accordance with SLAs?
- In accordance with documentation?
- What are the remedies?
- Duration is for term of agreement . . .

Liability

- Remedies for lost or damaged data
- Breaches surrounding privacy, security
- Compliance with regulatory laws
- Termination Assistance
- Insurance

Other General Issues

- Jurisdictional Issues (virtualization and mult-tenancy)
- Bankruptcy (financial strength monitoring)
- M&A
- Vendor Cessation of Business
- Subcontracting
- Open source
- Force Majeure

Other General Issues

- Electronic Communications Privacy Act (ECPA)
- IP
- Contingency Planning
- Price Protection
- Data Migration
- Accounting/ Revenue Rec. Issues (control vs. no-control)
- U.S. Patriot Act

Conclusion

- The technology is ahead of the lawyers.
- The business models are still evolving.
- The contracts are still evolving.
- Regulation/Laws are on their way.
- Organizations like NIST along with vendors are working diligently to create standards.
- The business must choose the appropriate service and deployment models.

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

Legal Issues in the Cloud: A Case Study

Jason Epstein
211 Commerce Street
Suite 800
Nashville, Tennessee 37201
(615) 726-5575
jepstein@bakerdonelson.com