Cloud Computing: Legal and Privacy Issues

Dr. Johndavid Kerr and Dr. Kwok Teng

E-Leader Vietnam, January 3-5, 2011

I. Introduction

- Cloud Computing: Emerging Technology and Trend
- "Clouds" are "data centers" or "server farms" on which software and data can be remotely stored
- Industry best practices to-date use on-site servers on the user's premises
- Economic incentives for clouding:
  - a) lower costs
  - b) limited site-support
  - c) scalability
  - d) elasticity of resource demand and supply

Security and Risk

- Traditional layers of legal protection for on-site security protocols include licensing agreements, common law contracts, sharing agreements, Service Level Agreements, and international conventions
- In a clouding environment, these traditional layers of protection may not fully protect:
  - 1) trade secrets
  - 2) intellectual property (patents, trademarks, and copyrights)
  - 3) private, personal information shared in multitenancy environments by third-party providers

Security and Risk Cont.

- Service providers may not be able to fully protect end-users (customers) against the following types of risk:
  - 1) loss of governance
  - 2) lock-in (guarantee data, application and service portability
  - 3) isolation failure (failure of mechanisms separating storage, memory, routing)
  - 4) compliance risks (loss of industry certification by migrating to cloud)
  - 5) management interface compromise
  - 6) data protection risks for customers and providers
  - 7) insecure or incomplete data deletion
  - 8) malicious insider risk

(European Network and Information Security Agency, 2009)

Scope of Research and Work

- Research and identify areas of risk embedded in emerging technology of cloud computing by examining traditional layers of legal protection and business practices (industry "best practices")
- Collaborate on development and publication of industry white paper with World Wide Technology's virtualization team; Pentagon technology grant
- Compile survey statistics from Ernst & Young's list of corporate clientele, supplementing white paper with research findings and results from survey instrument
- Examine and analyze industry and academic feedback for publication in peer-reviewed journal(s)

Future Shock: "As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electricity and telephone utilities, will service individual homes and offices across the country."

-Leonard Kleinrock, 1969 (Chief scientist of ARPANET) which seeded the Internet

(Welch, 2000)

Service-Oriented Architecture (SOA)

- The U.S. National Institute of Standards and Technology (NIST) working definition of Cloud Computing: " . . . A pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or services provider interaction." (Sun Microsystems, 2009)

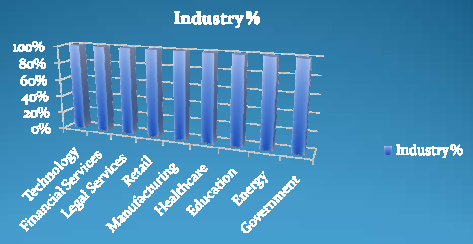
Industry growth & revenue projections

- Research firm IDC predicts global market for cloud services will reach $42 billion by 2012
- IDC also forecasts in its report that spending on clouding will accelerate, capturing 25% of IT spending growth in 2012, and nearly a third of growth in 2013
- ABI Research study predicts that cloud computing will change the mobile application world by 2014, generating a projected $20 billion in revenue

Source: (PhD Computing, 2009)

Cloud Computing: Industry Usage by Percentages

Source: Mimecast, 2010



Ontology model: architecture

(Youseff&DeSilva, 2009)

- Bottom layer: Hardware as a Service (HaaS)
  - physical hardware and firmware; subleased
  - backbone of the cloud
- Cloud software environmental layer
  - software platform layer
  - users are applications developers
  - Examples: Google's App Engine and SalesForce's Apex
- Infrastructure as a Service (IaaS)
  - computational resources, data storage, hardware-assisted virtualization

Architecture Cont.

- Software kernel
  - basic software management implemented as an OS kernel, hypervisor, virtual machine monitor and/ or clustering middleware
- Cloud application layer
  - most visible layer to the end-users of cloud
  - layer alleviates burden of software maintenance and ongoing operation and support costs

Three Service Models

(Cloud Computing, 2010)

- Software as a Service (SaaS)

a) most popular and common model

b) offers consumer online services and storage

c) rental of application functionality from a service provider instead of traditional approach of owning software (multi-tenancy environment)

Examples: Windows Live, Hotmail, Google Docs, Zoho and online business apps such as Salesforce.com

Service Models Cont.

- Platform as a Service (PaaS)

a) provides a platform in the cloud

b) model provides clients with a database management system, security services, workflow management, and applications serving

Examples: Google, Salesforce.com'sForce.com, Microsoft's Azure

Service Models Cont.

- Infrastructure as a Service (IaaS)

a) most basic level of the cloud

b) offers computer power and storage space on demand

c) clients are provided with full control of dedicated servers

Model leverages virtualization technologies: instead of running a virtual image on a partition existing on a physical service in a data center, the virtual image is spun on a virtual machine that has been created in the cloud

Risk Assessment & Management

- Cloud Computing is in its infancy (emerging trend)
- As illustrated, growing industry-wide demand for SOA and service provisioning models
- Customers range from small- to medium sized enterprises, and include MNCs
- In response to demand curve, small- to large-scale providers, contractors and subcontractors have created service models in public, private and community clouds
- Few industry-wide solutions to cloud computing risk

Risk Analysis: Studies & Reports

- Analyst firm Gartner's findings:

1) cloud computing is rife with security risks

2) inconsistent and non-uniform industry oversight on customer choices of qualified policy makers, architects, coders and operators, risk-control processes and technical mechanisms, as well as on the level of testing done to verify service and control process functioning

(Infoworld.com, 2008)

Gartner's findings

- Industry "best practices":

a) External audits and security verifications are traditionally required of service providers

b) Evidence was found that some cloud computing service providers refused to provide the required level of industry standardization and security scrutiny

- Mergers & Acquisitions (M&A):

a) High risk that data may not be available to customers if provider acquired by target suitor

b) High risk that data may not be in an importable format as to replacement application

Sarbanes-Oxley & Related Acts

- SAS-70 SOX compliance control objectives require a company to manage risk by ensuring that third-party processors place internal controls in their operations to ensure due diligence for audits and regulatory compliance:

-reasonable assurance that employees are aware of their responsibilities related to the confidentiality, integrity, and availability of data and information systems

-reasonable assurance that systems and services are available to customers in accordance with controlling SLAs

SOX & Related Acts (CB&H, 2010)

- reasonable assurance that installation of services are properly partitioned and configures to ensure contractual obligations are met

- reasonable assurance that confidential and/or personal client data including system access credentials are protected (e.g. encrypted) from unauthorized interception when transmitted over open networks (e.g., Internet)

- Gramm-Leach-Bliley Act, Payment Card Industry Data Security Standards (PSI DSS), and the Health Insurance Portability and Accountability Act (HIPAA)

Information Policy Trends in the United States

- Braman (2006) "Information policy in the United States, simply put, is continuing to fall further and further behind in policies related to new technology developments and how these developments are being employed. This gap between policy and technology has been noted, as has the increasing speed and distance of the gap as the U.S. continues to make laws retroactively and based on a pre-electronic mentality."
- Jaeger, Lin, and Grimes (2009) argue that to ensure the growth and adoption of cloud computing, it will be necessary to find technological and policy solutions for ensuring privacy and assuring information security.

Information Policy in the U.S.

- Federal Information Security Management Act (FISMA), Title III of E-Commerce Act of 2002:
  - uniform regime to address the levels of risk arising from domestic and international sources
  - information security is important to economic and national security interests of the U.S.
  - requires each federal agency to develop, document, and implement an agency-wide program to provide information security

FISMA Cont.

- Information security explained under the Act:
  1) for information and information systems that support the operations and assets of the agency
  2) including operations and assets provided by or managed by another agency, contractor or other source
- Cybersecurity – Act emphasizes a risk-based policy for cost-effective security

FISMA

- Requires agency programs officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of each agency's information security program and report results to Office of Management and Budget
- In FY 2008, federal agencies spent $6.2 billion securing the U.S. govt's total IT investment of approximately $68 billion or 9.2% of the total IT portfolio

Europe's Information Policy

- Sunosky (2000) One of the problems besetting the international community and WTO members is a set of different jurisdictional frameworks that offer varying levels of risk protection. The protection of personally identifiable information provides such an example—there are enormous differences between the minimal regulation of the United States and the intricate protection structures of the European Union

European Network and Information Security Agency (ENISA)

- EU governmental agency created to advance the functioning of the internal market and which produced a report in 2009 detailing the benefits, risks, and recommendations for information security
- Security Assessment: premised on three use-case scenarios:
  1) SME migration to cloud computing services
  2) impact of cloud computing on service resilience
  3) cloud computing in e-Government (e..g, eHealth)

ENISA: Security Risks

- Risks were tabulated according to the risk level as a function of the business impact and likelihood of the incident scenario, measuring risk on a scale of 0 to 8 against risk acceptance criteria
- Policy and Organizational Risk:
  - Experts identified as high risks lock-in, loss of governance (very high impact) and compliance challenges
  - Levels of risk may vary depending on provider and customer service level agreements and allocated cloud type: SaaS, PaaS, or IaaS

ENISA: Security Risks

- Technical Risks: high risks in isolation failure (very high impact, with medium probability in a public cloud), and cloud provider malicious insider (abuse of high privilege roles, including compromised intellectual property, personal sensitive data)
- Legal Risks: subpoena and e-discovery (risk of client/customer data through confiscation of physical hardware in criminal and civil suits); changes in jurisdiction (vulnerability: storage of date in multiple jurisdictions, lack of transparency about data storage, and data protection risks (reputation, personal data)

Legal Risks

- ENISA: SLAs govern the operational and procedural requirements associated with the pay-as-you-go costing arrangements per selected cloud type:
  a) govern "upstream" and "downstream" users in a clouding/on-demand model
  b) transfer risk during migration to cloud
  c) may be in conflict with promises made by other providers
  d) may carry too much business risk for a provider, given actual risk of technical failures
  e) CPs may have some rights to content stored on cloud infrastructure (e.g., IP content)

Legal Risks

- SLAs: users can negotiate terms and conditions on such important issues as perpetual licensing agreements, civil and criminal liability, fundamental breaches, data usage, proprietary scalability, and M&A protection and trailing liabilities (Spinola, 2009)
- Bargaining power between providers and end-users may be governed by standard contracts or individually-negotiated agreements (preferred method of liability protection because parties can tailor terms and conditions) (Nolan, 2009)

Global Trade & Liability Protection (Reed, 2010)

- World Trade Organization polices international trade between existing partners (147 countries)
- WTO's General Agreement on Tariffs and Trade (GATT) extends to new areas, such as service industries
- WTO expects countries to upgrade their IP laws to protect patents and copyrights and to guard against piracy of computer software
- Convention on International Sale of Goods (CISG) applies to international licenses and contracts (may preempt the UCC with adoptor-adoptee agreements

Strategies & Conclusion

- Mix of C-level and IT strategies must include frequent risk assessments and security "tests" by industry certified auditors
- Migration into a cloud transfers risk and SLAs and negotiated contracts must contain terms and conditions that protect against high levels of risk, such as lock-in, isolation failure, and M&A of providers by target suitor
- Board and corporate strategies must implement multijurisdictional policies and procedures, and must anticipate high legal, policy and operational risks in association with high-risk countries