Cloud Computing: Legal and Privacy Issues

September 15, 2010

Dr. Johndavid Kerr,
Assistant Professor of Business Administration
Harris-Stowe State University

Dr. Kwok Teng,
Associate Professor of Information Systems
University of West Alabama

Prepared for the Academy of Business Disciplines'
November 10-13, 2010, Conference
Ft. Myers, Florida

I. Introduction

Cloud computing, as an emerging technology and business trend, presents novel challenges to the traditional protections built into the law to ensure security of a corporation's proprietary resources, such as capital- and knowledge-based assets. Corporate counsel, C-levels, and stakeholders must understand that the traditional legal playing field is shifting, yet again, with the introduction of private and public clouds. These clouds are essentially "data centers" or "server farms" on which software and data can be remotely stored, instead of, for example, on a hard drive or on a server located on the user's premises. The economic incentives for cloud computing consist of lower costs, limited site-support, and "scalability," meaning that licenses and available resources can readily be adjusted to meet normal demand and supply curves.

Licensing agreements, contracts, sharing agreements, and *pro forma* documents may not provide adequate legal recourse and remedies normally associated with these layers of protection for corporations, and especially as applied to Small and Medium Enterprises ("SMEs"). And, this emerging trend presents a myriad of intellectual property, trade secret, foreign direct investment (FDI), and corporate governance risk issues that have yet to be fully explored, practiced or litigated in domestic and international markets and courts. There is also a prescient concern about privacy and protection of data from the standpoint of the cloud community, and about the ability of the service providers to ensure that privacy is not compromised and data is not lost or misappropriated. This concern will invariably factor into regulatory and governmental control and oversight as industries assess and reformulate the benefits inuring to cloud computing.

In light of the foregoing, this paper will address the technical, infrastructural challenges that cloud computing presents to traditional on-site computing, and will provide background information on the various protocols that are finding their way into cloud computing, such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and the like. In addition, the paper will examine the complex legal ramifications of traditional contractual protections afforded under civil law, and the uncertain legal landscape for Service Level Agreements and licensing arrangements under varying jurisdictional regimes. Under this examination, the paper will address some of the ethical challenges that are embedded in this emerging trend and its shifts toward private and public clouding. As the authors are working with the virtualization team at World Wide Technologies, a supply-side integrator with best-of-the-breed connections with Cisco, Dell Computers, VMWare, etc., this paper will be developed into a white paper as well.

II. What is Cloud Computing?

> *"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).*

This vision is here today, with backbone bandwidth in the Giga bits per second and the FCC's National Broadband Plan long-term goal of 100Mbs to the curb for all households (FCC DOC-296858A1, 2010). There are many definitions of Cloud Computing. The US National Institute of Standards and Technology's (NIST) working definitions captures the commonly agreed upon aspects 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 Microsystem 2009)*

They describe Cloud Computing using five *characteristics:* on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; *four deployment models:* Private cloud, Community cloud, Public cloud, Hybrid cloud; and *three service models:*

Software as a Service (SaaS). This is the most popular and common model, a consumer facing level that offers online services and storage. The approach here is the renting of application functionality from a service provider instead of the traditional approach of owning software. Examples include Windows Live, Hotmail, Google Docs, Zoho and online business apps like Salesforce.com, essentially delivering the equivalent of a complete application suite.

Platform as a Service (PaaS) – This model provides a platform in the cloud, upon which applications can be developed and executed. Google, again Salesforce.com (this time with Force.com), and Microsoft (with Azure) exist in this space (Schulz 2009; Cloud Computing). This model provided clients with a database management system, security services, workflow management, applications serving, and so on.

Infrastructure as a Service (IaaS). This is the most basic level of cloud computing, an offering of compute power and storage space on demand. Clients are provided with full control of dedicated instances of servers. This model leverages virtualization technologies. Rather than running a virtual image on a partition existing on a physical server in your data center, you spin it up on a virtual machine that you have created in the cloud. Virtual disks can be created in a similar manner to deal with the storage side of things (Cloud Computing). The vision of utility computing is based on the service-provisioning model like any other utility service; computing services will be readily available on demand (Buyya. *et al*.).

Cloud Computing is a new computing paradigm and is often synonymous with Cluster computing, Grid computing, Utility computing, P2P computing, Service computing, Market-oriented computing, and Web 2.0. and with the underlying technologies for implementing cloud computing. Some required characteristics of Cloud Computing are: It is highly reliable, very scalable, autonomic, ubiquitous access, and dynamic discovery (Buyya, *et al*.). This translates to a highly elastic and scalable pay-per-use computing model. Users, in essence, rent computing services as needed, deploy applications, store and access data all through Web 2.0 technologies, which translates into a scalable computing power at a much reduced cost structure.

In essence, Cloud Computing represents a shift from computing as a product that you buy to computing as a service that is provisioned to consumers/enterprise over the network from large-scale data centers or a “Cloud.” Cloud Computing is not about technological advances of the data centers, but represents a fundamental modeling change in how IT is provisioned and used.

In sum, the major driving forces of cloud computing are the shedding of capital and operating expenditures (servers, software, storage, networks, facilities, maintenance and administrative personnel) and provisioning an enormous amount of elastic (scale in/out) and ubiquitous (user just “plugs in” anytime, anywhere) buy-in for a range of applications and services.

As Cloud Computing technology has burgeoned and become more cost-efficient through the architectural changes and modifications of the above-discussed composite of varying models and their applications, there is a growing concern about another quickly developing area has matched the speed of Cloud Computing and that is the amount of risk or uncertainty inherently embedding itself in the layers of protection that have, up to this point in time, provided sufficient risk assessment and management controls and industry standards for on-site computing models.

III. Risk Assessment and Risk Management

As to industry forecasts about the economic benefits associated with cloud computing, the research firm IDC predicts the global market for cloud services will reach $42 billion by 2012. According to the same report, spending on cloud computing will accelerate throughout the forecast period, capturing 25% of IT spending growth in 2012 and nearly a third of growth the following year. An ABI Research study predicts that cloud computing will also change the face of the mobile application world by 2014, generating a projected $20 billion in revenue (PhD Computing, 2009). Even though the cloud computing industry is in its infancy and is largely driven by engineer-centric IT services, which evolved from grid computing, a predecessor to clouding, there is a growing demand for clouding services from customers ranging from SMEs to MNCs, and encompassing a broad range of service industries such as financial, telecommunications, healthcare, and legal services. Inherent within this service-based industry are multiple layers of low- to high-risk areas in connection with clouding types, such as Software as a Service (SaaS), Plaftform as a Service (PaaS), and Infrastructure as a Service (IaaS). In response to this demand curve, numerous small- to large-scale providers and ancillary third-party contractors and subcontractors have created a myriad of pay-as-you-go services in public, private and community clouds, with varying levels of expertise and resources and with varying levels of risk. Subsequently, as with any emerging technology and business model, there are few industry-wide solutions to cloud computing risks.

In its June 2008 report, the analyst firm Gartner released its findings that cloud computing is rife with security risks, challenging customers to ask vendors about the qualifications of policy makers, architects, coders and operators, risk-control processes and technical mechanisms, as well as the level of testing done to verify that service and control processes are functioning (Infoworld.com, 2008).

For example, on the issue of regulatory compliance, Gartner establishes that customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Gartner goes on to say that industry “best practices” require traditional service providers to undergo external audits and security certifications, cautioning customers to veer away from providers who refuse to provide this level of industry standardization and security scrutiny.

As to Mergers and Acquisitions (M&A) in a target scenario in which a cloud computing provider is acquired, for example, Gardner advises customers to find out if their data will be available after such an event, and if it would be in a format that could be imported into a replacement application (Infoworld.com, 2008).

A. Information Policy in the United States

To compound the complexity of these security issues, there is growing concern about a uniform information policy in the United States, with application to the emerging cloud computing technologies. 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 United States continues to make laws retroactively and based on a pre-electronic mentality (Braman, 2006). 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 (Jaeger, Lin, Grimes, 2009).

Youseff and De Silva (2008) established an "ontology model" to explain the virtualization layers in clouding: a) the physical hardware and firmware (subleased Hardware as a Service (HaaS), the bottom layer or backbone of the cloud); b) cloud software environmental layer (second layer: the software platform layer, users of this layer are cloud applications' developers, with examples such as Google's App Engine and SalesForce Apex); c) cloud software infrastructure layer (computational resources, data storage, and communications, including paravirtualization and hardware-assisted virtualization); d) software kernel (basic software management implemented as an OS kernel, hypervisor, virtual machine monitor and/or clustering middleware); and e) cloud application layer (most visible layer to the end-users of the cloud, this layer alleviates the burden of software maintenance and ongoing operation and support costs).

Despite the advantages of this clouding model, Youseff and De Silva (2008) recognize that deployment issues such as security and availability of the cloud applications are major issues that do not have an industry-wide solution yet. They further state that the leniency of SLAs may prolong a solution to these extant problems due to the composability of the clouding layered environment. Current security approaches include using Public Key Infrastructure (PKI) and X.509 SSL certificates as a methodology for authentication and authorization in the cloud. Youseff and De Silva opine that due to the absence of cloud computing standards, such issues as cloud security, data privacy and ownership policies will continue to be major concerns as a result of different approaches and services provided by each cloud provider.

The gaps between policies and technological realities are becoming so significant in some cases that arguments can be made that information policies may have to be completely rethought (Travis, 2006). This situation is further confounded by the number of policy decisions left to the marketplace in the United States that are more heavily regulated through policy in other nations (Jaegar, Lin, and Grimes, 2009).

In highlighting the case for a uniform and national information policy regime, Cloud Computing not only affects SAS-70 and Sarbanes-Oxley (SOX) compliance, but also Gramm-Leach-Bliley (GLBA), Payment Card Industry Data Security Standards (PSI DSS), and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with such regulations and standards requires varying degrees of security, and the data will likely need to be handled differently (CB&H, 2010).

An examination of the SAS-70 SOX compliance control objectives reveals the importance of managing risk by ensuring that third-party processors place internal controls in their framework to ensure due diligence for audits and industry and regulatory compliance. These regulations provide a global transparency of accepted accounting practices and standards, and telepath the industry’s commitment to corporate sustainability.   These regulatory controls, covering such directives as records retention, disclosure, and privacy, provide, among others:

- 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 the controlling Service Level Agreements;
- reasonable assurance that installation of services are properly partitioned and configures to ensure contractual obligations are met; and,

- 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) (Id., 2010).

To understand the layers of federal legislation and regulations applying to information policy and internet use, the Federal Information Security Management Act ("FISMA"), 42 U.S.C. § 3541 *et seq*., a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002, provides a uniform regime to address the levels of risk that may arise from domestic and international sources. The act recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency’s information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. In FY 2008, federal agencies spent $6.2 billion securing the government’s total information technology investment of approximately $68 billion or about 9.2 percent of the total information technology portfolio (FIMSA Website, 2010). 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 (Sunosky, 2000).

B. European Union's Risk Assessment Study

The European Network and Information Security Agency (ENISA), a EU governmental agency created to advance the functioning of the internal market, produced a report detailing the agency's findings on the benefits, risks, and recommendations for information security (ENISA, p. 4, 2009). In this report, the expert panel's and editorial board's findings were premised on a security assessment based on three use-case scenarios: 1) SME migration to cloud computing services, 2) the impact of cloud computing on service resilience, and 3) cloud computing in e-Government (e.g., eHealth). Pursuant to these scenarios, the report identified ten security risks that may occur as a result of implementing cloud computing; these risks include loss of governance, lock-in (guarantee data, application and service portability), isolation failure (failure of mechanisms separating storage, memory, routing and even reputation between different tenants), compliance risks (risk to industry certification by migration to the cloud), management interface compromise, data protection risks for customers and providers, insecure or incomplete data deletion (inadequate wiping out of data), and malicious insider risk (ENISA, pp. 9-10, 2009). The report states that of the ten security risks, there is no prioritization of criticality. These 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 that could be evaluated against risk acceptance criteria (ENISA, p. 22, 2009).

Under Policy and Organizational Risks, as referenced above in the serialization of risks in cloud computing environments, the expert panel identified, as high risks, lock-in, loss of governance (very high impact), and compliance challenges. The panel points out that these levels of risk may vary depending on the provider-and-customer service level agreement and as to which cloud type the risk is allocated; that is, SaaS, PaaS, or IaaS. Under this analysis, supply chain failure was rated as a medium risk, with concern about vulnerabilities to lack of completeness and transparency in terms of use, and about affected assets such as company reputation, customer trust, personal sensitive data, and service delivery.

Under Technical risks, the panel identified high risks in the areas of 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). (ENISA, pp. 33-44, 2009)

Under Legal risks, the panel identified as high risk areas subpoena and e-discovery (risk of client/customer data as a result of the confiscation of physical hardware as a result of subpoena by law-enforcement agencies or civil suits), risk from changes of jurisdiction (vulnerability: storage of data in multiple jurisdictions and lack of transparency about these storage facts, as applied to high-risk countries), and data protection risks (company reputation, personal sensitive data).

The report also considered the risks associated with SLAs, since these agreements govern the operational and procedural requirements associated with pay-as-you-go costing arrangements per the selected cloud type, and inherently transfer risk during migration to the cloud environment. In effect, SLA clauses may also be in conflict with promises made by other clauses or clauses from other providers. Further, according to the report, SLAs may carry too much business risk for a provider, given the actual risk of technical failures. In short, there may be clauses that are detrimental to customer, in that the CP may have any rights to content stored on the cloud infrastructure, which may include intellectual property (ENISA, p. 58, 2009). As the report concludes, risk assessment should be a regular activity rather than an infrequent one.

IV. Service Level Agreements and Terms of Use

SLAs govern "upstream" and "downstream" users in a clouding/on-demand model, and therefore, users can negotiate terms and conditions on such important issues as perpetual licensing arrangements, civil and criminal liability, fundamental breaches, data usage, proprietary scalability, and M&A protection and trailing liabilities, among others (Spinola, 2009). Nolan (2009) advises clients, on negotiations with regard to the bargaining power between cloud providers and end-users, that contracts may be standard forms or individually negotiated, which is the preferred method of liability protection because the parties can tailor the terms and conditions appropriate to the level and degree of contractual obligations and performance (Nolan, 2009). As a practical consideration, small- to medium-sized businesses may not have the kind of leveraging power to enter into substantive negotiations, due to scale, size and resources, that larger-scale enterprises, such as MNCs, will typically possess in traditional contract negotiations, and this economic reality may affect a small- to medium-sized company's ability to protect against risk in a clouding environment.

As to the global marketplace and the ramifications of clouding providers providing services in international markets, clouding users must understand the importance of various treaties and foreign government laws and regulatory regimes in considering what mix of IT and C-level strategies will work in the areas of risk assessment and management. Due to the emerging technology clouding markets, governments of both developed and developing countries are still responding to this SOA model by augmenting existing information and security policy(s) to include the SOA and quality of service (QoS) issues, resulting in a reactive, heterogonous framework of policies.

Under the World Trade Organization (WTO) existing tariffs are reduced and the agreement extends General Agreement on Tariffs and Trade (GATT) to new areas, including service industries. The WTO expects countries to upgrade their intellectual property (IP) laws to protect patents and copyrights and to guard against the piracy of items such as computer software and videotapes.   International licenses and contracts are recognized by and given protection under the Convention on the International Sale of Goods ("CISG") The CISG applies to contracts for the commercial sale of goods (consumer sale for personal, family, or household use are excluded) between parties whose businesses are located in different nations. If a commercial seller or buyer in the U.S., for example, contracts for the sale of goods with a company located in another country that has also adopted the CISG, the convention and not the UCC applies to the transaction (Reed, 2010).

As yet another example of the inherent difficulty of policing trade and security issues in a clouding environment, there arises a troubling set of questions about the scope and reach of the CISG's coverage of SLAs across multijurisdictional lines, which includes the implications of what rules of law apply and in which forums and venues such disputes can be resolved. These issues, as suggested earlier, may have to be ultimately resolved through litigation and its appeal cycles before a final determination on the allocation of risk(s) can be made and before a bright-line test(s) on these issues can be drawn. The importance of regional alliances to comparative advantage also needs to be considered in these risk assessments, as there are numerous alliances that, in some cases, have restricted trade solely to their member states, affecting the clouding community's ability to protect against levels of risks present in such jurisdictions.

The North Carolina Bar Association recently crafted a proposed Formal Ethics Opinion in connection with the propriety of using a practice management program (e.g., Clio) in the practice of law. Under the Rules of Professional Conduct ("RPC"), a law firm may use such a cloud computing program provided that steps are taken to minimize risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including file information, from risk of loss. The proposed rules were crafted in cooperation with and oversight from the ABA Legal Technology Resource Center, whose leadership provided guidance and counsel on the merits of cloud computing. The proposed Opinion includes advice to lawyers and law firms on such specifics as: a) what is the history of the SaaS vendor? b) where does it derive funding? c) Has the lawyer read the user or License Agreement terms, including the security policy, and does he/she understanding the meaning of the terms? d) Does the SaaS vendor's Terms of Service or Service Level Agreement address confidentiality? If not, would the service vendor be willing to sign a confidentiality agreement in keeping with the lawyer's professional responsibilities? Would the vendor be willing to include a provision in the agreement stating that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect client information? and, e) Where is the data hosted? Is it in a country with less rigorous protections against unlawful search and seizure? (Mazzone, 2010).

Industry-wide data, according to a cloud computing adoption survey conducted by Mimecast.com, revealed that out of 565 respondents across the United States and Canada, the top adopters of cloud industry are Technology (53% using the cloud), Financial Services (41%), and Legal Services (37%). Included in the survey were Retail (35%), Manufacturing (32%), Healthcare (32%), Education (29%), Energy (24%), and Government (19%). Survey respondents (70% of those using cloud technology) indicated that they were planning to move additional applications to the cloud, with 83 percent doing so in the next 12 months (Mimecast, 2010).

V. Conclusion

Based on the foregoing discussion, cloud computing is an emerging technology and flexible business model in which inherent layers of risk exist throughout the value chain. The industry-wide adoption and utilization of industry certifications and security measures remove some of the risk by implementing internal controls and ensuring password and encryption measures; however, due to the lack of uniformity present in the terms and conditions of provider contracts and Service Level Agreements, as discussed, consumers may be exposed to layers of risk depending on how much risk of loss is assumed by the providers, subcontracting third-party vendors, and other parties included in the liability chain. As shown, governments have not provided a uniform and homogenous information policy regime in which private industry is given clear guidance as to multijurisdictional risk, cyberterrorism risk, outage risks, and M&A risks. The European Union's ENISA 2009 report finds that the highest areas of risk can be found in policy and organization risks, technical risks, and legal risks. International trade and law regimes, through a lacework of laws, regulations, and treaties, and while providing some legal protection and recourse for contracts, intellectual property, and trade secrets, do not have a protective umbrella of civil and criminal liability that coordinates on information policy, jurisdiction conflicts, inconsistent application of laws, and divergent political and economic systems.

Thus, the traditional system of contractual protection afforded service industries, such as financial, technological, and healthcare industries, may be exposed to high levels of risk by entering into Terms of Use agreements and Service Level Agreements in which providers hold the upper-hand on assumption of liability and risk of loss, as defined in negotiations and final calls. In this environment, SMEs may be at a disadvantage due to lessened leverage and power to negotiate, in comparison to larger enterprises, such as MNCs, whose ability to negotiate more favorable terms and conditions is predicated on more scalable resources and more layered protections against the levels of risk in cloud computing technology. As such, each organization must conduct a thorough and diligent risk assessment of the potential threats of low to high risk inherent in cloud computing environments, and must ensure that all management and operational strategies and initiatives incorporate an optimal mix of cost-efficient processes, policies, and controls to mitigate against these risks.

References

Braman, S. (2006). *Change of state: Information, policy, and power.* (Cambridge: MIT Press).

Brodkin, Jon. Gartner: Seven cloud-computing security risks. Retrieved on March 26, 2010 from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

Buyya, R; Yeo, C.S., and Venugopal, S.. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Retrived September 21, 2010 from http://www.buyya.com/papers/hpcc2008_keynote_cloudcomputing.pdf.

Cloud Computing, SAAS - IAAS – PAAS. Retrieved September 21, 2010 from http://www.vdcon.net/pch/CLOUD_COMPUTING.html.

Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Network and Information Security Agency (ENISA) Report. Retrieved on February 3, 2010 from http://www.enisa.europa.eu/.

Federal Information Security Management Act, 42 U.S.C. ("FISMA"), 42 U.S.C. § 3541, et seq.), Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). Retrieved on September 8, 2010 from http://csrc.nist.gov/groups/SMA/fisma/index.html.

FCC DOC-296858A1, 2010, http://hraunfoss.fcc.gov/edocs_public/index.do?document=296858.

Jaeger, P.T., Lin, J., and Grimes, J. Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information and Politics*, 5(3): 269-283, 2008.

Khajeh-Hosseini, A., Sommerville, I. and Sriram, I. Research Challenges for Enterprise Cloud Computing. Retrieved on September 21, 2010 from http://arxiv.org/abs/1001.3257.

Mazzone, Eric, Director of Center for Practice Management, North Carolina Bar Association, (in e-mail communications with counsel to the Ethics Committee, 3/30/10 and 3/31/10) and ABA Legal Resource Technology Center. Retrieved on September 12, 2010 from http://www.goclio.com.

Mimecast Unified E-mail Management, *Cloud Computing Adoption Survey, 2010*. Retrieved on February 3, 2010 from www.Mimecast.com.

Nolan, P. (2009). Partner Cloud Computing: The Legal Issues.

Reed, O.L., Shedd, P., *et al.* The Legal and Regulatory Environment of Business, 15th Edition (2010 McGraw-Hill-Irwin).

Schulz, Wayne, 2009, What is SaaS, Cloud Computing, PaaS and IaaS? Retrieved on September 20, 2010 from http://www.s-consult.com/2009/08/04/what-is-saas-cloud-computing-paas-and-iaas/.

Spinola, Maria, An Essential Guide to Possibilities and Risks of Cloud Computing. Retrieved on March 31, 2010 from http://www.mariaspinola.com/whitepapers/Updates_White_Paper_An_Essential_Guide_to_Possibilities_and_Risks_of_Cloud_Computing.html.

Sun Microsystems, Introduction to Cloud Computing Architecture, 2009.

Sunosky, J.T. (2000). Privacy online: A primer on the European Union's Directive and the United States' Safe Harbor privacy principles. *Currents: International Trade Law Journal*, 9, 80-88.

The Impact of Cloud Computing on SAS-70 Compliance Issues, Cherry, Bakaert & Holland L.L.P. Retrieved on September 13, 2010 from http://www.cbh.com/index.asp.

Travis, H. (2006). Building universal digital libraries: An agenda for copyright reform. *Pepperdine Law Review*, 33, 761-833.

Understanding Cloud Computing, A white paper for executives making decisions on computing resources, Executive Summary. Retrieved on May 20, 2010 from http://www.phdcomputing.net.

Youseff, L., Butrico, M. and Da Silva, D. Toward a Unified Ontology of Cloud Computing. Retrieved on March 26, 2010 from http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf.

Welch, Matt. BIRTH OF A BLUEPRINT**:** Profile Internet Father, Leonard Kleinrock The Zone News January 2000. Retrieved September 19, 20101 from http://www.mattwelch.com/ZoneSave/Kleinrock.htm.