Information Security Management in Cloud Computing and Mobile Technologies

by

Fernando A de Almeida
dealmeidaf12@students.ecu.edu
East Carolina University
College of Technology & Computer Science
Department of Technology Systems
Information Security Management

Table of Contents

Abstract

Recent trend in popularity of cloud and mobile computing can be explained as the result of technology enabling technology through constant innovation (Ernst & Young, 2012, p. 2). Individual users and companies are gradually incorporating cloud and mobile technologies in their IT solutions. Gartner Newsroom (2010) predicts the "industry is poised for strong growth through 2014 when worldwide cloud services revenue is projected to reach $148.8 billion" (p. 1). This trend moves simultaneously with the shift of personal information from homes and private data centers into third-party providers. This new reality requires information security professionals to educate users and their own teams balancing functional access to data versus control mechanisms to guarantee availability, integrity and confidentiality of information.

This research of literature is concerned with unique aspects of management of information security applied to cloud and mobile technologies. It was conceived under the premise that there is increasing risk when organizations and individuals rely on mobility and cloud computing services.

This review starts by defining cloud and mobile computing along with popular architectures and services. It investigates strengths and weaknesses of both technologies from the perspective of services built over them and security capabilities they offer. The research concludes with assessment of public and private initiatives to reduce uncertainty in risk level and promote sustainable evolution of mobile computing solutions.

Keywords: mobile cloud computing, cloud computing services, mobile technology, mobile security, Cloud information security, the law and cloud computing

Introduction

Business and individuals rely on timely access to information to remain competitive, monitor events in real time or just maintain contact with family and friends. Smartphones, laptops and tablet computers are enablers of this new wave of data exchange and have become tools of preference for daily interaction among millions of users around the world (Kottari, Kamath, Saldanha, & Mohan, 2013). Powered by mobile communications and cloud resources data is constantly on the move adjusting to workforce needs, capacity management or just to improve performance bringing source and destination as close as possible to minimize access latency.

Driven primarily by economic reasons corporate and personal data are gradually shifting away from private control into hybrid and public clouds. Data hosted by third-party providers, outside customer premises, face challenges from exposure to new threats to eventually losing protection under the Law. As the industry embraces new applications for mobile communication, information technology (IT) and information security (IS) professionals update the Information Security Governance adding new controls into the process. This constant update of strategic, tactical and operational planning is needed to guarantee alignment of information security and business objectives, update risk management, and support business case showing the value of investment in security.

The lack of full control when data is in transit or in the cloud forces IS/IT managers to reconsider traditional SLAs looking for more liability from providers; better understanding of locations and uses of data centers; capacity management that could off-load data across borders, and impact cloud locations may have on Federal, State and local jurisdictions.

This research recognizes the new data management paradigm and calls attention to items that must be addressed when IT/IS managers formulate strategic and operational plans involving mobile and cloud computing.

Deployment And Service Models In The Cloud

The Cloud was conceived as a services oriented architecture that came to life triggered by advances in virtualization at server, application and networks. According to the U.S. National Institute of Standards and Technology (NIST), Mell & Grance (2011), Cloud computing is:

> … a model for enabling ubiquitous, 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. This Cloud model promotes availability and is composed of five essential characteristics, three service model, and four deployment models (p. 2).

Service models over the cloud are defined as: Software as a service (SaaS) that describes the application layer where users can access commercially available software only paying for the

service they need rather than purchasing licenses; platform as a service (PaaS) aimed at hosting home grown applications. Infrastructure as a service (IaaS) to make available virtual resources that can be rented such as CPU, storage, network access, memory, etc.

There are four cloud computing deployment models: private cloud, community cloud, public cloud and hybrid cloud. Private cloud offers better control as it is dedicated to a particular organization. It tends to face fewer threats as compared to public or hybrid architectures. Community cloud similarly to private cloud offers some level of control. It is built for communities of interest sharing similar requirements and concerns. Public cloud, as the name says, is open to multiple uses and consumers. It offers flexibility and low cost and operates under less stringent controls. Hybrid cloud offers a combination of features from other deployment models (Mell & Grance, 2011). Each model is conceived balancing security, privacy, cost and control.

Cloud computing is changing the way computing resources are perceived and incorporated into any IT business cycle. Report from Tech America Foundation (2011), Cloud First, Cloud Fast, sees cloud technologies redefining the way computing power is acquired and used; particularly with strong appeal to cost savings, efficiencies and innovation.

The Cloud has been implemented all over the world via proprietary and sometimes through open standards. Openstack.org for instance, is an open source platform, it offers shared engine with no vendor lock-in. VMWare, Amazon and Microsoft Azure are based on proprietary platforms.

Mobile Technologies

Market trends have shown that mobility adds efficiency when information is needed anytime and anywhere. Smartphones, laptops and tablets are probably the most popular devices incorporating mobility features offering full range of capabilities. Mobile devices access information in real time from multiple sources dispersed logically and geographically. Adoption of mobile communication has become popular making the technology attractive targets for malware and other mechanisms aiming at breaching security (La Polla, Martinelli & Sgandurra, 2012). The ecosystem of mobile applications tends to reside remotely in the cloud creating a unique scenario where there is constant communication between mobile device and server resources.

Mobile operating systems such as MS Windows Mobile from Microsoft, iOS from Apple, Symbian OS, Blackberry OS used by Research In Motion and Android from Google are comprehensive in capabilities and have vulnerabilities the same way as general purpose operating systems in laptops, workstations and servers. From a transport perspective devices such as smartphones or tablets support multiple standards. La Polla (2012), addresses wireless standards such as IEEE 802.11, Global Systems for Mobile Communications (GSM) and Bluetooth, just to name a few, that are easily integrated with Internet Protocol (IP). This type of integration gives mobile devices full access to immense array of upper layer applications ranging from banking to eCommerce, health care, social networking and more.

Popular mobile and cloud services relying on Google (Google App Engine/BigQuery Service/Cloud Storage/Gmail), Amazon (EC2), Microsoft (Web Apps/Azure Platform/Live

Meeting), Oracle (ERP), Salesforce.com (CRM) and Citrix (XenMobile /XenServer) among others are great fit for mobile devices. Those services are not immune from virus, Trojans, rootkits, botnets among many threats that can come into the enterprise via mobile access. La Polla (2012), provides a comprehensive list of mobile malware including type, operating system and effect the malware has on information confidentiality, availability and integrity.

Mobile applications and operating systems have own application programming interfaces (APIs) for better integration with each other and with remote systems. Gradually mobile devices tend to rely more on remote resources in the cloud for CPU (processing), storage, etc., minimizing demand on local devices.

Service Level Agreements And Performance Indicators

The literature shows no consistency on how key performance metrics and service levels are adopted across mobile communication and cloud computing providers. A summary of key performance indicators from the perspective of users when choosing the best fit cloud hosting provider is described by (Sangha, 2013). The same author also describes KPIs from the perspective of users of cloud services. The listing by Sangha (2013) gives generic pointers to areas of discussion to be negotiated into custom service level agreements (SLAs).

From (Sangha, 2013) here are key performance indicators (KPIs) that buyers should consider when evaluating providers …

- Featured Services: Quality of featured services and metrics
- Cost of Featured Services: Basic vs. Premium vs. Tiered
- Performance: Service vs. Platform metrics
- Availability: Uptime Metrics
- Risk Management: Incident response and management metrics
- Support: Basic vs. Premium & Live help vs. Online
- Cloud Service Provider Financial Viability

Not mentioned by Sangha (2013) is transparency with regards to hiring practices and overall compliance with auditing to demonstrate controls safeguarding data confidentiality and integrity.

(Amazon.com, 2013) service level agreement for the EC2 cloud services product offering is available in their website and is very much in line with the industry. Most providers of cloud and mobile communications tend to limit their liabilities due to service incidents with little to no transparency on how the business is run other than commitments on availability measured by uptime percentage. Providers offer service credits in case performance metric “uptime” is not met. Another example where” uptime” is used as performance indicator is in the SLA offered for Google family of services including cloud storage, Google prediction API, and Google BigQuery (Google, 2013). Similarly to Amazon, Google restricts liability commitment to

measuring and reporting on "uptime" data. (Rackspace, 2013) in item 17 of their Cloud Terms of Service stipulates "Limitation on Damages" even in the presence of gross negligence or willful misconduct by the provider.

Another interesting perspective on service agreements in mobile services is as seen in (Verizon, 2013). It appears there is commitment to give to the customer a limited amount of credits in case of service interruption. In (AT&T, 2013) we see very similar approach offering to the wireless customer compensation via service credits in case of outages. There is no commitment on security. Other major wireless providers adopt similar agreements.

Is this approach to customer service agreement enough to assure data confidentiality, integrity and availability in the mobile and cloud environments?

What service transparency is offered to consumers? How important are SLAs for services for mobile and cloud services?

TechAmerica Foundation (2011) summary report has identified the need for better metrics and disclosure when dealing with services over the cloud. Lack of consistent mechanism via tools and metrics to evaluate performance of providers leave users somewhat exposed. Calloway (2010) calls attention to the danger of click-wrap service agreements. Acceptances of such agreements by users give to providers dangerous waivers in liability when dealing with data and information protection. An example was given where click-wrap contract allowed UPS to limit liability to $100 after losing a package worth $105,000. What happens if your business is sharing the environment with business that breaks the law? Are you at the risk of indirectly suffering consequences due to someone else sharing physical space in the virtual environment?

Adoption of best practices is a constant topic when debating growth of cloud and mobile computing. Levi & Riedel, 2010, list the following US regulations and standards, among others, containing "provisions relating to the storage, protection, or transfer of data and require that relevant data and/or operations be auditable": Sarbanes-Oxley Act of 2002 (SOX), Pub. L. 107-204, Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. article 3541, et seq. These standards are now part of the integrated world of technology and law where compliance is mandatory. Levi, 2010, illustrates the impact the regulations and standards listed above have on business survivability when companies have to produce evidence in court cases.

Security Concerns In Cloud And Mobile Technologies

Armbrust et al. (2009), identified ten potential obstacles to growth of cloud computing. Availability, one of the key pillars in information security, was listed as key decision element when users are considering cloud solutions. The concern with availability is followed by concerns with data lock-in, data confidentiality and auditability, data transfer bottlenecks, scalable storage, bugs in large-scale distributed systems, scaling quickly, reputation fate sharing and software licensing.

Cloud computing capitalizing on benefits of virtualization and concentration of information increases the risk to information protection (CSA, 2010). Any breach of security on a cloud environment pays more dividends to perpetrators and has the potential to amplify harm. This has not gone unnoticed by the hacker community according to (Sturmer, 2013).

Survey by the Cloud Security Alliance, (CSA, 2010) and work by Intel assessing security best practices in cloud services, (Intel, 2012) are summarized below. The list highlights key data protection concerns raised by users and providers of cloud services:

1. Abuse and nefarious use of cloud services. Cybercriminals actively target cloud services providers due to relatively weak registration system to access cloud services and potential for high return on their efforts. According to CSA (2010), "by abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity" (p. 8). Examples of abuse according to CSA (2012) are: "IaaS offerings that have hosted the Zeus botnet, InfoStealer Trojan horses, and downloads for Microsoft Office and Adobe PDF exploits" (p. 8). "Botnets that have used IaaS servers for command and control functions. Spam continues to be a problem – as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist" (p. 8).
2. Insecure APIs. According to Intel (2012) APIs are important application-layer control for protecting against data loss, threat protection, and other content-delivered attacks. In addition APIs are key for organizations and third parties to offer value-added services to their customers according to CSA (2010). Securing API integrity is paramount on security strategy.
3. Malicious insiders. CSA (2010) indicates the malicious insider problem arises when providers have little to no transparency into their hiring practices. They do not reveal how cloud access is granted to employees, monitoring safeguards that have been implemented or business practices to review logs for policy compliance.
4. Shared technology issues. Intel (2012), "Even with virtualization hypervisor to mediate access between guest operating systems and physical resources, there is concern that attackers can gain unauthorized access and control of underlying platform with software-only isolation mechanisms" (p. 5). Example of this exploits is in Kortchinksy (2009) CloudBurst presentation. Covert channels can be created besides other potential exploits.
5. Data loss/leakage. Data loss scenario for example is when data is encrypted and keys are lost rendering it unrecoverable. Another scenario is when data is in common hardware and confiscated due to fate sharing. Jurisdiction issues could be a problem where data is placed outside the expected jurisdiction or unavailable due to confiscation. This is a huge point of concern as control moves into provider's hands.
6. Account or service hijacking. CSA (2010) lists phishing, fraud, and exploitation of software vulnerabilities as the means to succeed stealing access through account or service hijacking.
7. Unknown risk profile. The lack of transparency among cloud service providers creates a grey area preventing required in-depth analysis consequently hiding the true risk profile.

Concerns listed in bullets 1 to 7 above serve go guide any proactive strategic and operational security planning. In item number 4 the issue of shared resources was introduced. What makes

it a security concern? Providers of cloud computing services try to maximize return on investment by multiplexing as many customer virtual machines (VMs) as possible across shared infrastructure. Kortchisnky (2009), raises concerns about bugs and leaks present in virtualization code and architecture. These deficiencies are capable of introducing exploits in cloud environments. Kortchisnky (2009), illustrates his point through the use of examples based on VMware vulnerabilities. Ristenpart, Tromer, Shacham & Savage (2009), take advantage of initial flaws in the Amazon EC2 service to describe how hackers could map virtual machines in a Cloud infrastructure with the goal to identify potential targets. Their paper emphasizes how to instantiate new VMs co-residing with targets with intend to take advantage of exploits.

Sharing physical resources even through virtualization can be dangerous. This is known as reputation fate-sharing. One can be blacklisted if sharing blocks of IPs or can have data confiscated in case of court's decision affecting the shared resource. From a services perspective mobile and cloud technologies move control away from user and into provider's facilities. This meaning control over data is shared and sometimes transferred to provider. The issue can be aggravated depending on service and deployment models raising the requirement for security mitigation techniques (Subashini & Kavitha, 2010). How can we enforce regular auditing in provider facilities? Would they agree with it? What about other tenants? The issue can get really complicated.

In item 2 concerns with APIs were briefly introduced. What makes API management an important component of the security plan? APIs are critical at all levels. APIs are offered by vendors to facilitate interface between applications, applications and operating systems and between operating systems. In the cloud APIs are used to interface with hypervisors, build, configure or decommission virtual machines. Any vulnerability either on APIs or software that makes use of them can become source of exploits by hackers and malicious users in general. Mather, Kumaraswamy & Latif (2009) give an example of zero-day vulnerability in HyperVM made by Lyxlabs that allowed damage to 100,000 websites hosted by an UK based company called Vaserv.com. Through the exploit hackers were able to run UNIX commands forcing recursive delete of files.

In mobile computing we see similar concerns with control over data and eventual losses. APIs can be compromised, mobile devices can be lost or stolen or just hacked into. According to CSA (2012) users of mobile technology have identified the following top security concerns: "

- Data loss from lost, stolen or decommissioned devices
- Information-stealing mobile malware
- Data loss and data leakage through poorly written third-party apps
- Vulnerabilities within devices, OS, design and third-party applications
- Unsecured WiFi, network access and rogue access points
- Unsecured or rogue marketplaces
- Insufficient management tools, capabilities and access to APIs
- NFC and proximity-based hacking "

Common threats and vulnerabilities identified in mobile devices (enumerated below) explain concerns by users listed in CSA (2012) survey. A list of aggregated vulnerabilities and threats facing mobile devices is summarized below:

- Lack of Physical Security Controls: As the function indicates mobile devices tend to be remote and connect to internal and external networks in multiple locations and across jurisdictions. Encryption techniques along with balanced user education programs are mandatory steps in improving security when mobile devices are part of active enterprise inventory.
- Use of Untrusted Mobile Devices: There are many mobile devices out there, multiple manufacturers, security posture, and cutting edge IT innovative strategies such as "bring your own device", BYOD. The recommended approach according to (Souppaya & Scarfone, 2013) is to consider mobile devices as untrusted entities in the Enterprise. BYOD while bringing pros and cons to business (Chellakari, 2012) are considered an outsider component and care should be given to such devices as information technology professionals define the line between functionality and access.
- Strong encryption of data in mobile devices is considered mandatory best practice.
- Untrusted Applications: NIST has multiple recommendations on how to deal with untrusted applications. They go from blocking such applications to performing specific risk management for each new untrusted app acceptable by the business. Basically the IT and IS professionals have to review return on investment to justify risk and measures to protect the technology.
- Interaction with Other Systems: There are many scenarios under which a mobile device can function as gateway into the Enterprise. Each scenario should be carefully evaluated to avoid establishing accidental backdoors. Tethering systems (untrusted laptop via smartphone into Enterprise perimeter) is a good example of device interaction with potential for backdoor.
- Untrusted Content: Any means of introducing untrusted content needs to be evaluated and access decided. User education is still a key factor in effectiveness when dealing with content.
- Location Services: According to (Souppaya & Scarfone, 2013), overall recommendation is to turn off or opt out of location services, mainly if location is considered sensitive information for your organization. While there are other mechanisms that could expose location of mobile devices (ex. public IPv4 IP used without application proxy), location services tends to be the location revealing method with most exposure.

Initiatives To Secure Mobile And Cloud Computing

Risk in mobile communications has been summarized by Milligan & Hutcheson (2007), as a basket of threats starting with malware written specifically to mobile, potential theft of valuable data, over the air sniffing and tethering through lack of access controls. Mobile technology serves as one of primary gateways into the cloud. Concerns raised by Milligan & Hutcheson, 2007, addressing mobile technology still remain relevant. Technology evolves and as it happens the risk factor needs to be readjusted to account for new threats. To identify ways to understand and address risk industry leaders, user groups and government are joining forces to standardize

the environment. For instance, Intel is working with other technology makers to define standards and reinforce layers of security protecting vital components of the cloud (Intel, 2012). The mobile industry and user groups are standardizing as well particularly demanding support to secure communication.

Best practices in the industry recommend creating custom secure images of virtual machines and applications. Create strong inventory control and protect the images considered safe to install including the library of APIs. Hardening services, strong access control, passwords, patching and file system monitoring are among traditional methods that equally apply to mobile and cloud communication. Enterprises should develop and enforce policies (NIST SP 800-124rev1) in addition to establishing strong identity management programs.

Intel (2012) offered the following planning steps as way to mitigate information security problems when data is on the move:

Step 1: Start security planning early. It requires a comprehensive review of intended usage of mobile and cloud communication starting with self-assessment questions such as location of compute resources. This assessment will permit identify if regulatory compliance is required.

Step 2: Identify vulnerabilities in your cloud environment. Intel (2012) recommends review of the new security perimeter redefined by cloud computing.

Step 3: Mitigation strategies. Intel (2012) recommends relying on encryption techniques to safeguard data. Encryption implies strong key management strategy at file level.

Step 4: Protect data in motion, in process and at rest. As listed in step 3, the key to protecting data on the move or at rest is cryptography. Strong encryption seems to have broad acceptance as effective risk mitigation strategy.

Step 5: Secure your platform. The concern by Intel (2012) is to prevent placement of threats such as rootkit and other low-level.

Intel (2012) lists three enforcement points that can provide critical layers of protection for any platform and infrastructure: " a) Client security that ensures only authorized users can access the Cloud; b) Controls at the API level where external software interacts with the cloud environment; c) Hardware-based technologies that build trust between servers and between servers and clients " (p. 16). The above can be facilitated by strong Identity and Access Management initiative covering users, client and servers in the cloud (Subashini & Kavitha, 2010).

Step 6: Enable compliance monitoring. The recommendation is to select service providers that offer basic compliance with industry best practices that incorporate monitoring and accountability. Per Intel (2012) "Acts such as the Federal Risk and Authorization Management Program (FedRAMP) in the United States and the Data Protection Act in the United Kingdom" (p. 4) often requires security enforcement and can create audit needs.

Step 7: Choose the right cloud service provider. Be aware of their controls, including location of premises and negotiate SLAs.

When selecting the services provider one has to look at access control to data and resources, auditability and compliance with regulatory standards (even the most generic/basic ones).

Mobile devices such as smartphones and tablets are all about the apps, mostly interacting with resources and data in the cloud. As mobile devices reach into public and private business they extend traditional IT perimeter. Souppaya & Scarfone (2013), have issued and released NIST special publication 800-124 revision 1 defining new guidelines for managing mobile devices when brought in as part of the Enterprise. These guidelines try to respond to industry and user concerns about information protection in mobile devices. The NIST guideline capitalizes on best practices and other NIST publications for comprehensive view of mobility as part of the total IT inventory of equipment and services. Souppaya & Scarfone (2013) offer mitigation strategies to make information security planning more robust. A summary based on NIST SP 800-124 rev 1 recommendation from Souppaya & Scarfone (2013) is shown below:

- Mobile device security policy: Make mobile security part of the systems security clearly defining which devices are accessed via mobile technology.
- Develop system threat models for mobile devices indicating resources that are accessed through them. By doing so it becomes easier to visualize and validate controls needed to mitigate risk.
- Review security and control features of mobile devices allowed in the Enterprise. The NIST SP 800-124 rev1 recommends adopting mobile solutions that facilitate implementing remote security controls. If mobile devices interact with cloud (public or private) make it possible remotely enforcing use of encryption, strong passwords and device authentication. Restrict the user only to applications approved by IT. Prevent downloading and installation of untrusted apps in any mobile device.
- Establish a pilot implementation to close gaps: Pilot implementation can be seen as industry best practices prior to rolling into production any new change or technology. During pilot phase the IT organization side by side with functional groups have the opportunity to fine tune strategy and controls required in the mobile solution. The pilot is an opportunity for discovering and learning.
- Establish baseline before allowing user access to mobile devices: This means create and approved a trusted image per mobile platform. Lock down the device and then give it to the user. The intent is to raise the level of comfort the organization has with each device knowing they comply with standard corporate implementation.
- Develop long term plan for mobile security strategy. This can be accomplished by having strong change management process and procedures. ITIL framework for transition to operations and change control can be a good reference point.

The recommendation above works through planning and enforcement. It relies on constant verification of compliance with processes and procedures defining the organization's core activities. Certification and accreditation of processes supplemented by periodic audits is the recommended way to maintain control over the secure environment.

In the European Union the Cloud Security Alliance has led many efforts to provide guidelines for standardizing security in cloud computing. The European Network and Information Security Agency (ENISA) issues publications and promote initiatives on securing the cloud and mobile communications. (Enisa, 2013) discusses mobile identify management along with typical threats, security risks, best practices and recommendations to mitigate exposure in the mobile environment.

Across the literature it appears there is concentrated awareness and effort to secure mobile and cloud as they become extended perimeter of any IT infrastructure.

The Law When Data Is On The Move

Privacy laws need special attention particularly when data crosses jurisdictions. The Electronic Communications Privacy Act of 1986 (ECPA), codified under title 18 of the U.S.C. was enacted to account for transmissions of electronic data by computer expanding original wire taps (Department of Justice, 2012).

Stored Communications Act (SCA), "codified under title 18 of the U.S.C. chapter 11, sections 2701-2712, is a law that addresses voluntary and compelled disclosure of stored wire and electronic communication and transactional records held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act (ECPA)". This component of the law is extremely important when deciding what type of data can traverse mobile and cloud computing environment. Certain data may be allowed into public clouds replicated anywhere. Other type of data may require private cloud with data centers located within a particular law jurisdiction (Federal / State / Local).

With regards to ECPA and SCA, Keswani (2011), highlights vulnerabilities that organizations face when deciding for storing sensitive information in the cloud. Management of warrant requirements to obtain electronic data, Stored Communications Act 18 U.S.C. section 2701-12 (SCA), stored in the cloud (mobile apps) is perceived by the courts as transferred to a third party. According to SCA, legal steps to obtain data held by third party are less stringent than if the same data were retained in computers kept at home or private data center. This issue has been recently debated in the US Congress showing indication that current law may change.

With regards to international data transfers, Lakatos (2012) calls attention to fears that many in the industry inside and outside USA, have of undesired exposure of information to the US government. The Patriot Act as a tool expands existing mechanisms available to law enforcement to reach into personal data. The Patriot Act including Foreign Intelligence Surveillance Acts (FISA) warrants and National Security Letters (NSL) are seen as powerful instruments in the hands of the government. Data gathering activity is protected by the Patriot Act only if to assist prevention of foreign intelligence activity or protection against terrorist plots toward U.S.A. Kushida, Murray & Zysman (2011) bring forward additional questions related to the reach of the Patriot Act.

The U.S.-EU Safe Harbor framework was created to facilitate mutual understanding of protection of personal data (export.gov, 2012). Iqbal et al. (2010), summarizes core issues related to multi-jurisdiction with regards to data on the move, particularly cloud computing.

Conclusion

Mobile and cloud solutions are highly scalable, capable of responding to fast roll-out of services and can be sold on demand. Do advances in mobile and cloud based applications create new paradigm in data protection? The literature suggests the answer is yes, they do. Technology moves fast sometimes ahead of laws and controls designed when less capability was available.

Many Internet based services are now leveraging mobile and cloud computing for cost efficiency and productivity. Key providers such as Salesforce.com, Google, Yahoo, Microsoft, Amazon.com and Terremark are leading the effort offering more control through innovation on services. Key providers of cloud technology such as Intel, VMware, Microsoft are also introducing control features in their products to facilitate securing information on the move. The concern about lack of specific metrics in SLAs as far as commitments to safeguarding information in the cloud still persists (Messmer, 2013).

Fear of unreasonable exposure without protection was validated when Gmail failure hit 160,000 users after a software upgrade causing account deletions as mentioned in work done by Calloway (2010). In the presence of gross-negligence limited liability clauses in SLAs may not hold, but still creates risk of loss for the user. Evaluating your provider's capabilities including ability to commit to SLAs is essential in risk assessment.

Service and deployment models in mobile computing and cloud have extended traditional perimeter of security. The threat of liabilities and weak controls emphasizes the need for comprehensive planning from strategic, tactical and operational viewpoints.

Combining all initiatives by private and public organizations we see mobile and cloud gaining space in mainstream business. There is still plenty of work to be done. The right technologies along with solid planning for data protection can elevate the confidence level leading to universal adoption of cloud and mobile technologies.

References

Ernst & Young. (2013). *View from the top. Global technology trends and performance. Issue 10*. Retrieved from http://www.ey.com/Publication/vwLUAssets/View_from_the_top_-_Global_technology_trends_and_performance_-_October_2012_-_February_2013/$FILE/View_from_the_top_Global_technology_trends_and_performance_October_2012_February_2013.pdf

Gartner Newsroom (2010). *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010*. *Gartner*. Retrieved from http://www.gartner.com/it/page.jsp?id=1389313

Kottari, V., Kamath, V., Saldanha, L.P., Mohan, C. (2013). *A Survey on Mobile Cloud Computing: Concept, Applications and Challenges*. IJAIR Vol. 2 Issue 3. Retrieved from: https://s3.amazonaws.com/academia.edu.documents/31067670/A_Survey_on_Mobile_Cloud_Computing Concept__Applications_and_Challenges.pdf?AWSAccessKeyId=AKIAIR6FSIMDFXPEERSA&Expires=1372967830&Signature=IdP%2BnbFBWm8SQTkfwUkMRNAqxkg%3D&response-content-disposition=inline

Mell, P., Grance, T. (2011, September). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology, Special Publication 800-145. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

TechAmerica Foundation. (2011). *Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation*. Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD2). Retrieved from http://www.techamericafoundation.org/cloud-commission

La Polla, M., Martinelli, F., Sgandurra, D. (2012). *A Survey on Security for Mobile Devices*. IEEE Communications Surveys & Tutorials. Retrieved from: http://www.iit.cnr.it/sites/default/files/A%20survey%20on%20Security%20for%20mobile%20devices.pdf

Sangha, H. (2012, March 28). *KPI's for Cloud Service Providers & Customers*. Cloud Computing. CloudTweaks. Retrieved from http://www.cloudtweaks.com/2012/03/kpis-for-cloud-service-providers-customers/

Amazon.com (2013). *Amazon EC2 Service Level Agreement*. Retrieved from http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf

Google.com (2013). *Google Cloud Storage, Google Prediction API, and Google BigQuery SLA*. Retrieved from https://developers.google.com/storage/docs/sla

Rackspace. (2013). *The Rackspace Cloud Terms of Service*. Retrieved from: http://www.rackspace.com/cloud/legal/#LimitationonDamages

Verizon (2013). *Customer Agreement & Important Information*. Retrieved from http://yourguide.vzw.com/legal/customer-agreement/

AT&T (2013). *Wireless Customer Agreement*. Retrieved from http://www.att.com/shop/en/legalterms.html?toskey=wirelessCustomerAgreement-list

TechAmerica Foundation. (2011). *Summary Report of the Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD2).* Retrieved from: http://www.techamericafoundation.org/content/wp-content/uploads/2011/07/CLOUD2_Summary.pdf

Calloway, T.J. (2010). *Cloud Computing, Clickwrap Agreements, and Limitations On Liability Clauses: A Perfect Storm*? DUKE Law & Technology Review. Retrieved from: http://dltr.law.duke.edu/2012/03/30/cloud-computing-clickwrap-agreements-and-limitation-on-liability-clauses-a-perfect-storm/

Levi, S.D., Riedel, C. (2010, March 01). *Cloud Computing: Understanding the Business and Legal Issues*. Practical Law Company. Retrieved from http://us.practicallaw.com/8-501-5479

Armbrust, M., Fox, Al., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M. (2009, February 10). *Above the clouds: a Berkeley view of Cloud computing*, Technical report, Electrical Engineering and Computer Sciences, University of California at Berkeley. Technical Report No. UCB/EECS-2009-28. Retrieved from: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

CSA Cloud Security Alliance (2010, March). *Top Threats to Cloud Computing v1.0*. Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Sturmer, J. (2013, March 28). *Hackers follow business shift to cloud computing*. ABC.News. Retrieved from http://www.abc.net.au/news/2013-03-27/cloud-security/4598036

Intel IT Center. (2012, September). *Planning Guide Cloud Security Guide. Seven Steps for Building Security in the Cloud from the Ground Up*. Retrieved from http://www.intel.com/content/dam/www/public/us/en/documents/guides/cloud-security-checklist-planning-guide.pd

Cloud Security Alliance (CSA). (2012). *Top Threats to Mobile Computing*. Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/mobile/top_threats_mobile_CSA.pdf

Kortchinsky, K. (2009) *Cloudburst—a VMware guest to host escape story*. Black Hat USA 2009.

Ristenpart, T., Tromer, E., Shacham, H., Savage, S. (2009). *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.

Subashini S, Kavitha V. (2010). *A survey on security issues in service delivery models of Cloud computing*. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.07.006

Mather, T., Kumaraswamy S., Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. Sebastopol, CA: O'Reilly Media, Inc.

Souppaya, M., Scarfone, K. (2013, June). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Institute of Standards and Technology, Special Publication 800-124 Revision 1. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Milligan, P.M., Hutcheson, D. (2007). *Business Risks and Security Assessment for Mobile Devices*. Retrieved from: http://www.wseas.us/elibrary/conferences/2007vancouver/papers/558-187.pdf

Chellakari, K. (2012). *Developing a BYOD Strategy: Weigh the Risks, Challenges and Benefits*. Retrieved from: http://searchsecurity.techtarget.com/feature/Developing-a-BYOD-Strategy-Weigh-the-Risks-Challenges-and-Benefits

Enisa, European Network and Information Security Agency. (2013). *Mobile Identity Management*. Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/Mobile%20IDM

U.S. Department of Justice (DOJ). (2012). *Federal Statutes. Electronic Communications Privacy Act of 1986 (ECPA)*. Office of Justice Programs, Justice Information Sharing. Retrieved from http://www.it.ojp.gov/default.aspx?area=privacy&page=1285#contentTop

Keswani, A. (2011). *Community Economic Development in the Cloud: How Low-Cost Technology Is Democratizing Development and Driving Community Growth*. Journal of Affordable Housing & Community Development Law. Retrieved from: https://login.cyrano.ucmo.edu/login?url=http://search.proquest.com/docview/1019052328?accountid=6143

Lakatos, A.C. (2012, January 18). *The USA Patriot Act and the Privacy of Data Stored in the Cloud*. MAYER*BROWN. Retrieved from

http://www.mayerbrown.com/publications/The-USA-Patriot-Act-and-the-Privacy-of-Data-Stored-in-the-Cloud-01-18-2012/

Kushida, K. E., Murray, J., Zysman, J. (2011, June 03). *Diffusing the Cloud: Cloud Computing and Implications for Public Policy*. Springer. Journal of Industry, Competition and Trade. Retrieved from: http://brie.berkeley.edu/publications/WP_197%20update%206.13.11.pdf

Export.gov. (2012). *U.S.-E.U. Safe Harbor*. Retrieved from http://export.gov/safeharbor/eu/eg_main_018476.asp

Iqbal, A., Black, B., Fisher, C., Cella, J., Abrams, J., Dugi, M., Leventhal, R., (2010). *Cloud Computing & National Security Law*. The Harvard Law National Security Research Group. Retrieved from: http://harvard.academia.edu/AatifIqbal/Papers/523189/CLOUD_COMPUTING_and_NATIONAL_SECURITY_LAW

Messmer, E. (2013, April 10). *Gartner: Long hard climb to high level of cloud computing security*. NetworkWorld. Retrieved from https://www.networkworld.com/news/2013/041013-gartner-cloud-security-268587.html?page=1

McKendrick, J. (2011, November 11). *Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward*. Forbes. Retrieved from http://www.forbes.com/sites/joemckendrick/2011/11/20/cloud-computings-vendor-lock-in-problem-why-the-industry-is-taking-a-step-backwards/

American Psychological Association (APA) Style. *Purdue Online Writing Lab*. Retrieved from http://owl.english.purdue.edu/owl/resource/560/1/

Federal Trade Commission. (2011, March 30). *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network.* Retrieved from http://www.ftc.gov/opa/2011/03/google.shtm

Verizon. (2012). *Data Breach Investigations Report (DBIR)*. Retrieved from: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S. (2011, September). *A Survey on Security issues in Cloud Computing.* Retrived from http://www.tifr.res.in/~sanyal/papers/Survey_on_Security_Issues_in_Cloud_Computing_and_Associated_Mitigation_Techniques.pdf

Trappler, T. (2010). *If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues*. Retrieved from: http://www.educause.edu/ero/article/if-its-cloud-get-it-paper-cloud-computing-contract-issues

Kandukuri, B. R., Paturi, R. ,Rakshit A. (2009). *Cloud Security Issues*. In: IEEEinternational conference on services computing, 2009, p.517–20. Retrieved from http://xml.csie.ntnu.edu.tw/JSPWiki/attach/Supergud/Cloud%20Security%20Issues.pdf

NIST, National Institute of Standards and Technology. (2012, May 16). *Detailed Overview. Federal Information Security Management Act (FISMA)*. Computer Security Division-Computer Security Resource Center. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

CA.gov. (2012). *Health Insurance Portability and Accountability Act*. California Department of Health Care Services. Retrieved from http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00%20WhatisHIPAA.aspx

U.S. Securities and Exchange Commission-USSEC. (2012, August 30). *Sarbanes-Oxley Act 2002*. The Laws That Govern the Securities Industry. Retrieved from http://www.sec.gov/about/laws.shtml#sox2002

Cox, P. A. (2011, March 11). *Mobile cloud computing: Devices, trends, issues, and the enabling technologies*. developerWorks. IBM. Retrieved from http://www.ibm.com/developerworks/cloud/library/cl-mobilecloudcomputing/

Cox, P. A. (2011, June 24). *Build a more secure, mobile cloud environment: Common mobile cloud vulnerabilities and solutions to secure them*. developerWorks. IBM. Retrieved from http://www.ibm.com/developerworks/cloud/library/cl-mobilecloudsecurity/

Samson, T. (2013). *9 top threats to cloud computing security*. Info World. Retrieved from https://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428?source=footer

Appendix

Definition of Terms

Broad network access – Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) (Mell & Grance, 2011).

Data lock-in – Proprietary implementations of Cloud computing that may prevent users from easily switch between vendors (McKendrick, 2011).

Google Docs – Web-based office suite and data storage service offered by Google.

HIPAA – Health Insurance Portability and Accountability Act of 1996. Among other things establish establishes national standards for electronic health care transactions and national identifiers for providers (CA.gov, 2012).

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider (Mell & Grance, 2011).

PCI DSS – Payment Card Industry Data Security Standard is an information security standard for organizations that handle cardholder information for the major debit, credit, etc. It provides actionable framework for developing secure process to handling personal information (PCI, 2012).

Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time (Mell & Grance, 2011).

Sarbanes-Oxley Act of 2002 (SOX) – It is a United States federal law to protect investors by improving the accuracy and reliability of corporate disclosures (USSEC, 2012).