iS
CHANNEL

Reshaping the Organizing Vision of Cloud Computing

How the Snowden Revelations Affected Stakeholder Action

Andrea Acs
MSc Management of Information Systems and Innovation (2013/2014)
Department of Management
London School of Economics and Political Science

KEYWORDS

Cloud Computing
Organizing Vision
Privacy
Snowden Revelations

ABSTRACT

The recent revelations of government surveillance in the United States by Edward Snowden have had a profound effect on attitudes towards and perceptions of privacy. Given that this area of technology is highly privacy-sensitive and that the market is dominated by US companies and their local subsidiaries, the Snowden revelations led to changing perceptions of privacy in the cloud business. Therefore, this research aims to provide a European perspective, and discusses how relevant stakeholders, namely regulators, adopting organizations, and suppliers are reacting. The author argues that the technology was before black-boxed with a strong, common understanding of its risks, benefits and regulations and a supporting organising vision, and that this box is now being opened and stirred up as a result.

Introduction

Cloud computing has been one of the most prominent buzzwords in Information Technology circles in the past few years. Encompassing a wide range of services from web-based software to access to remote computing infrastructure, the term has been used as an umbrella to make sense of this emerging phenomenon. A commonly used definition for cloud computing is "remotely available service of utility computing via data center hard- and software" (Armrbust et al., 2010). Service models of cloud computing take many shapes, the most common categorization being Infrastructure (IaaS), Platform (PaaS) and Software as a Service (SaaS). cloud computing's complexity therefore lies in its diversity, as well as in its newness.

Theoretical Frameworks

In order for an innovation to be widely adopted and diffused, a common understanding of the underlying technology is needed. The concept of *organising vision* introduced by Swanson and Ramiller (1997) provides a useful perspective on how the cloud computing market was formed, and eventually, changed after learning about the actions of the U.S. intelligence agencies.

The goal of *organising vision* is to explain how "a collective, cognitive view of new technologies enables success in IS innovation both within and across firms" (Swanson and Ramiller, 1997). The discourse around the innovation is shaped by all members of community, and is often characterized by buzzwords. Furthermore, the authors state, "information systems innovation cannot simply be extrapolated from new technology, but rather, willfully cast in images of the future, quite literally, imagined".

The process to reach a shared organising vision within the community includes three steps: *interpretation*, *legitimation* and *mobilization*. *Interpretation* is the exploratory process to provide a broadly shared account and provide institutional coherence; while *legitimation* is the process through which the underlying rationale is developed and the innovation gets grounded in broader business concerns. Thereafter, *mobilization* is there to facilitate exchange and structure market sources. (Swanson and Ramiller, 1997)

The framework of organizing vision is particularly useful to provide an account of cloud computing because it takes into consideration the multiple constituencies and accounts for how their discourse shapes the understanding of an innovation. Applying this theory helps us investigate how institutional forces shape the uptake of technology and how individual actors make sense of it, contrary to earlier research that views innovation as a local, rational choice (Swanson and Ramiller, 1997). This lends understanding to how the phenomenon of cloud computing as a buzzword is formed with taking into the perspectives of suppliers, customers and regulators.

The process of forming an organizational vision has

Corresponding Author
Email Address: A.Acs@lse.ac.uk (A. Acs)

been at a quite mature stage up until recently with participants having gone through all three stages and forming a stable view. However, as forming an *organising vision* is deeply grounded in practice and discourse and is dynamic, events that I will discuss in Part 2 have not only shaped, but also disrupted the process.

Another way to look at the cloud landscape is through what Galliers et al. (2001) call the supplier perspective. By black-boxing it, the industry often presents technology as a simple fix for organizational problems. In order to do so, they "conceal the complexity of the underpinning knowledge to allow for rapid diffusion." (ibid .)

And indeed, the rhetoric surrounding technology focused on the business benefits of flexibility, on-demand use and scalability, a service-like cost structure and management benefits of transparency and the ability to focus on one's core business. Above all, the technological promise that location does not matter, as also suggested by the label 'cloud', has become the strongest selling point (Grimes et al., 2009). However, as the authors call to our attention, "the cloud itself is an abstraction and is used to represent the Internet and all its complexity" (ibid). The black-box of cloud computing therefore has been effectively communicated, with regulation in place and risks seemingly well-understood by adopters. As a result, industry discourse remained focused on how cloud adoption makes perfect business sense in the public and private sectors.

After discussing in more detail how cloud computing was understood by major stakeholders, Part 2 discusses the actions that disrupted it, and Part 3 explains how major stakeholders reacted to newly make sense of the situation. Thereafter, in Part 4, I discuss how a new *organising vision* is in the making.

Part 1: Perspectives before Snowden

Corporate Perspective

The cloud computing market in Europe seems strong and growing. Gartner estimates the worldwide public cloud services market to reach 131 billion US dollars in 2013, with Western Europe being the second biggest market, bringing in 24% of this revenue (van der Meulen and Rivera, 2013). Major business benefits are commonly seen in enhancing efficiency and speed through variability and scalability; a pay-per-use structure that aids understanding of IT costs; as well as a tool for innovation (Venters and Whitley, 2012a).

On the flip side, security and privacy have always been the major issues preventing faster adoption of cloud computing. Especially from an IT executive's perspective, security, off-shore data housing, lock-in and compliance are the top four concerns (Venters and Whitley, 2012b), three of which can be associated with data protection issues. Others, however, argue that cloud computing can mitigate these risks by better management of hardware and skills, as well as more effective responses due to scale effects (ibid).

Technology Perspective

In order to understand the reality of cloud computing adoption, it is crucial to understand the technology that drives and enables it. In parallel to the perception of potential cloud users I discussed above, the most significant challenge of the technology is to ensure security. In Xiao and Xiao's model, the ecosystem of cloud security and privacy consists of defense, threats and vulnerabilities, which influence its two major pillars. One pillar of how security is dealt with in the cloud concerns the users' business needs (e.g. integrity, availability, confidentiality and accountability (Xiao and Xiao, 2013)). These themselves are strongly intertwined with privacy concerns. The other pillar is privacy, which the authors acknowledge to be highly relevant to security.

Similarly, the National Institute of Standards and Technology, a major technology regulatory body defines the key issues to be multi-tenancy, trust, encryption and compliance (Mell, 2009). *Multi-tenancy* is one of the major enablers of hardware utilization, through placing the data of multiple, often anti-cyclical businesses' data on one physical server and making it accessible through virtualization (Xiao and Xiao, 2013). This of course does not mean that customers can access each other's data, but increases the cloud's vulnerability. For example, should hackers target one organization, it might have a spillover effect on others.

Trust refers to relinquishing control over the protection of the data (Grance and Jansen, 2011), and entrusting that the third party not only has the benevolence, but also that they have the relevant skills for risk and security management, that insiders cannot abuse the data and that the data stays under the ownership of the data controller.

Encryption is a commonly used technique to address the issues of unjustified access by the provider's employees or those associated with multi-tenancy (Xiao and Xiao, 2013). Encryption before the data leaves the company's premises and storage in the cloud is thought to be an efficient way to ensure confidentiality and integrity (ibid.). Alternatively, firms can choose to replace corporate identifiers with anonymous data before it leaves company firewalls (Venters and Whitley, 2012b).

Compliance is the organization's ability to operate in agreement with established laws, regulations and standards (Jansen and Grance, 2011). Of particular relevance for compliance is the physical location of the data, which is a technical, strategic and political issue all at once. Many regulations require data to stay within the borders of a given jurisdiction, while suppliers are often reluctant to disclose data center locations, often claiming that it is technically not possible given the ubiquitous nature of cloud computing. Academics closer to the matter argue against this, given that providers need to be aware of that information in order to, among others, access data and bill customers (Whitley, 2014a).

Regulatory Perspective

The major regulation that governs the processing of personal data and transborder flows, and therefore is highly relevant to the use of cloud computing, is the EU's Data Protection Directive, translated into national legislation by member states (Whitley, 2014b). According to the Directive, personal data is "any information relating to an identified or identifiable natural person (*'data subject'*); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity ". It also clearly defines the responsibility of the *'data controller'*, the company users entrust their data with, to safeguard it and ensure appropriate measures taken in its protection, such as ensuring that the data is not transferred to countries the European Commission does not judge as providing "an adequate level of protection". It is the cloud customer's (who is legally the *data controller*) responsibility to ensure that the cloud provider, the *data processor*, does not transfer the data to any other countries than those of the European Economic Area, Brazil, Argentina, Canada (Whitley, 2014b).

As an extension, an agreement between the European Commission and the US Department of Commerce, the Safe Harbour Principles, provide an opportunity for US-based service providers to acquire certification. Through this mechanism, companies compliant with the EU's principles in the above-mentioned European directive, such as Apple and Google, are allowed to process personal data of EU citizens (export.go, n.d.), which should provide sufficient protection if combined with binding corporate rules (King and Raja, 2013). Therefore, it is compliant with regulations for the European subsidiaries of these companies to store the backup data of their clients in the United States to ensure geo-redundancy (Whittaker, 2011).

The issues addressed by such regulations are not limited to cloud computing, indeed, many of them were formulated before its existence. The dynamic and global nature of the cloud, however, make sourcing such services more complicated. One problem is that vendors have data centers in multiple jurisdictions as well as often further outsource to subcontractors (Whitley, 2014b). Privacy protection therefore might not be guaranteed to an adequate level. Another, maybe even more pressing, issue is concerned with physically locating the data. It is, however, questionable whether cloud providers are able and willing to disclose data locations (Clarke and Svantesson, 2010).

Part 2: Events Leading to Changes in Understanding Concerns before Snowden

Based on what I discussed in Part 1, I believe there was a common understanding in the marketplace about what cloud computing is, what its benefits and risks are, and how to mitigate them. I argue that a series of recent events has had a profound influence on this understanding and ultimately led to opening up the Black Box.

In 2001, the United States introduced the Patriot Act, which regulates wiretapping and the access to stored electronic communications. And while the law provides some protections for US citizens, for example through the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008, foreigners such as European citizens, are left vulnerable (Whitley, 2014b).

The press widely discussed how this impacts the rights of individuals, its relevance to cloud computing went largely unnoticed (Zorz, 2013) with many assuming that the above-discussed Safe Harbour provisions provide adequate protection (Whitley, 2014b). Eventually, the public learned that this is not the case. Microsoft came forward first in 2011 admitting that being a US-based company, if the National Security Agency (NSA) instructs them, they are forced to give out information stored in their clouds (Whittaker, 2011b). Not only is this contrary to the rules of the European Union, which they are also obligated to adhere to, they are also often restricted from informing the affected companies or individuals.

The Snowden Revelations

The major blow, however, came in 2013 when Edward Snowden came forward, leaking information to The Guardian about the PRISM program that provides the NSA direct access to the servers of the likes of Apple, Google and Facebook (Greenwald and MacAskill, 2013). While many were already uneasy about the Patriot Act allowing for surveillance of individuals approved by secret courts, it was now that the world learned that the USA is conducting mass-surveillance on individuals in the name of national security, but without any direct reason to do so. The Snowden documents also revealed that encryption, the major safeguard of Internet privacy, has been also broken by the NSA by tinkering with the underlying cryptography (Larson et al., 2013).

The stream of leaked documents not only stirred conflict between the United States and the rest of the world, but also within the European Union. The GCHQ, the British counterpart of the NSA, is said to be collaborating with the NSA. The Guardian reported that in the operation codenamed Tempora, GCHQ is able to tap the fibre optic cables, thereby collecting and storing huge amounts of online and telephone data (Ball et al., 2013). The UK being one of the major Internet hubs within Europe, this goes way beyond compromising data of only UK citizens.

Given the small number of US companies that dominate the global cloud computing market, these events have the potential to fundamentally change our understanding and attitude towards such services. The implications to European cloud customers are threefold. For one, companies having cloud contracts with US-based providers, or more commonly their local subsidiaries now have to reinvestigate whether

they are compliant with existing EU regulations, as well as keep up with the potentially changing ones. Secondly, beyond compliance issues, they have to consider additional measures to safeguard data from the US government's prying eyes. Since information in the cloud is often not just private but also business critical, it is also the responsibility of cloud customers to safeguard their and their economies' competitiveness, should the US government decide to use it for other reasons than protecting national security. Lastly, given that vast amounts of aggregated data is collected and stored by the NSA, as well as encryption potentially being compromised, cloud customers now have to reconsider whether they are safe from malicious individuals, organizations and even competitors.

What are the alternatives to just deciding to hold back on cloud adoption? While we thought that location matters little, now we learn that there is a need for a more Europe-focused approach to cloud computing. Part 3 discusses how major European stakeholders, namely governments and the EU, corporate customers and vendors have reacted to alleviate a situation and form a new organizing vision.

Part 3: Reactions

Governments and Regulators

"It would be a sad outcome of the surveillance disclosures if they led to an approach to Internet policy-making and governance in which countries became a series of walled gardens with governments holding the keys to locked gates." John F. Kerry, general counsel of the United States Commerce Department (Hakim, 2013)

And indeed, what Kerry fears seems to come true to at least some extent. National governments, as well as European institutions like the European Commission have responded swiftly to the events, both in rhetoric and in action. European leaders urged for the development of a European Network. The German chancellor, Angela Merkel, for example, called for an NSA-proof Internet in Europe. On the other hand, she also acknowledged that there are still national differences and until common ground is found, nations have to seek their own solutions (Clark, 2014).

The European Parliament is addressing the regulatory gap by updating the digital privacy regulation, which now includes explicit rules about cloud computing (Hakim, 2013). The amendments proposed include the data controllers having to notify subjects, should their data be moved outside of the EU (European Parliament, 2013). In the case of cloud computing, where data in bulks is in question, this may very well be prohibitive. The European Commission is also working on introducing significant sanctions on companies that turn over data to law enforcement authorities in ways that violate European privacy regulations (Hakim, 2013; Tielmans, 2014).

Moreover, the Commission is in conversation with US authorities regarding the major issues to be addressed considering the Safe Harbour Agreement. They claim that the massive collection by US authorities goes behind what is proportionate and necessary. The agreement failed to provide the purpose it was originally designed for, namely to provide higher, European protection standards for personal data in the United States (Reding, 2014). The EC has given concrete recommendations for the US authorities to address, mainly in the areas of transparency, possibility of effective redress, effective enforcement and limitations of access by public authorities (ibid.).

Meanwhile, fixing regulation is just the tip of the iceberg. Many see an opportunity in keeping the data within the European region. One way to go about that is to build national clouds (eg. the made-in-France initiative cited by Darrow, 2012), which might not be beneficial. In a 2013 memo, the European Commission expressed being strongly against so-called "Fortress Europe" approaches, as actions based on national rules could prevent the free flow of data even within the EU. They also acknowledge that slowing adaption of cloud computing is hurting European business' (especially SMEs') competitiveness. Therefore, the European Commission's strategy for "unleashing the potential for cloud computing in Europe" (European Commission, 2012) and thereby creating a single, European market, gained attention, speed and relevance since the Snowden revelations. Actions are taken on several fronts: updating unified data protection rules, building a single market and building standards and certification schemes for EU cloud providers.

This is not just a possibility to mitigate the current issues, but also provide a business opportunity for the region and European vendors. In the Commission's interpretations, there are three pillars to that. Most importantly, Europe is famous for high data protection standards. This could serve as a competitive advantage and help Europe become the world's most secure and trusted region for cloud computing. Secondly, a truly functioning European market would be big enough to achieve economies of scale. Lastly, they see the Public Sector as an early adapter, thereby driving further cloud growth (European Commission, 2013).

A slightly more radical measure, "Schengen for data" has also appeared in the news recently. Referring to the EU's free travel zone, the proposal includes a data routing system that would allow for data to stay within on the European continent. Significantly, the United Kingdom, whose intelligence agency, GCHQ, is said to be cooperating with the NSA, is not part of the Schengen zone and therefore could also be bypassed. However, experts find the idea very costly and largely ineffective, since it would not be of any use when people use websites from outside of Europe, such as Facebook (Seiffert, 2014).

Customers

"If our systems ran on Amazon's cloud in the Netherlands and it went down as a result of a technical issue, we would have to shut business down before the backup came live in

the United States. We can't afford that." IT Manager for a major UK-based retailer

And indeed, many customers think similarly. In a survey of corporate customers, the Cloud Security Alliance asked non-US customers how the Snowden incident affected their cloud sourcing strategy (Cloud Security Alliance, 2013a). They found that 10% of respondents cancelled projects with US-based providers in response to the Snowden incident, while 56% claim that they are less likely to use them in the future.

Although privacy and compliance have always been among the biggest obstacles to cloud adoption (Willcocks et al., 2012) at least there has been a relatively clear understanding of what these were. Indeed, since the regulation within the European Union is currently in constant flux, companies might even have difficulties understanding what rules they have to comply with. The lack of transparency leads to difficulties in risk assessment (Whitley, 2014b) and as a result, potential customers struggle to make decisions based on what makes business sense.

Therefore, it becomes ever more important for corporations to structure ways of assessing risks. Pearson for example argues that privacy is much more than a compliance issue and that privacy considerations have to be part of designing cloud computing services (Pearson, 2009). He argues the Privacy Impact Assessments should be initiated early in the design phase and repeated in all stages and provides different solutions to mitigating risks identified throughout. A more recent form of addressing risks in a timely manner is to seek vendors that provide Privacy Level Agreements (PLAs), besides the traditional Service Level Agreements (SLAs). In same document, the CSA also stresses the importance of internal due diligence, namely reviewing the company's own security measures and potential privacy threats; and external due diligence, such as finding a provider with relevant certifications and understanding whether the customer will have the ability to see and control security at the vendor. (Cloud Security Alliance, 2013b)

Given the lack of major, Europe-based alternatives, some consider running private clouds and hope to realize at least some of the business benefits. Experts, among others the European Commission, warn, however, that on-premises solutions are not completely secure either. They "lack the ability to call on high levels of professional security" such as effective authentication and state of the art security implementation, which cloud provisioning with the right specifications could provide (European Commission, 2013).

Vendors

"Repeatedly we see companies saying we're the ones out there on the front lines defending this, ... U.S. companies can't solve this problem, and that's the biggest challenge right now." Daniel Castro (as cited in Corbin, 2014)

While Europe accounts for 24% of the global cloud computing market, only 8% of the vendors are European (Armbrust et al, 2010). Clearly, the dominant US-based players are aiming to keep their market-leading position despite the growing mistrust and harder compliance. At the same time, European companies are to grab the opportunity and position themselves in the reshaping marketplace.

Some intend to pacify users through disclosing information beyond what they are required to. Google, for example, recently published a Transparency Report that details how often they were approached by authorities with requests for data, and the proportion of which they fulfilled (Google, 2014). Others, such as IBM, are hoping to increase their footprint by investing in new data centers (IBM, 2014). However, that only provides a solution once the legitimacy of Safe Harbour is back in place.

As a recent study of the cloud infrastructure market shows, location sensitivity, as expected, is a major decisional factor for European customers (Miller, 2014). In particular, a survey of hosting providers found that local knowledge, presence, cultural fit and an existing customer base contribute to successful cloud services (Armbrust et al, 2010). That understanding, combined with the mistrust of US providers and the European Union's efforts to foster European cloud computing, one should expect local players to gain greater presence.

Given the recent nature of this issue and the slower pace of the corporate world, the first new, European or local providers are to be seen in the consumer market. Examples include Younited*, a Dropbox alternative in Finland and "E-mail made in Germany", a cooperative initiative of German ISP providers and telecoms (Juskalian, 2014). In the corporate world, we see some established providers trying to gain attention through using their European identity, such as the Aruba cloud† listing four major selling points: price, performance, data center location in London and being part of the European data center network.

If we are looking for hard numbers, the most relevant study that is currently available is one carried out by the Information Technology and Innovation Foundation (ITIF). It predicts that US providers' share of the non-US market could fall as low as 55% by 2016 (Castro, 2013). In their analysis, they attribute this trend to falling trust post-PRISM, as well as to Europe's actions for data protection and building their own cloud network.

Part 4: Forming the New *Organising Vision*

The "European Cloud"

In this article, I have shown how cloud computing and its risks were thought of, and thereafter discussed what events have influenced this understanding. I argue that before the recent events, there was a

* http://www.younited.com/
† http://www.arubacloud.com/home.aspx

specific vision, and market participants shared a story of what risks and dangers were. While previously, the three stages of forming an *organising vision* were close to completion; the recent events caused the process to restart. *Interpretation* is now again under way, with participants trying to grasp how they and their use of the technology are affected. Governments, regulators, companies and vendors have now restarted the discourse, with clients asking hard questions, and suppliers rushing to change their advertising rhetoric and offerings that better fit the current needs. These interactions are vital to reshaping each others' perspectives as well as to *initiate forming a new organizing vision.*

A new, more geography-focused understanding is formed through *legitimation.* New buzzwords, such as the "European Cloud" and "Schengen for Data" emerge, while corporations, vendors and regulators join to make sense of the new situation. Furthermore, since parties act upon it, for example by forming legislation or other changing their sourcing practices, one can also argue that *mobilization* is now also in progress.

Conclusion

In this article, I investigated how the Snowden revelations have affected the European cloud computing market in the past year. The European Union and its regulatory bodies busied themselves with updating data protection legislation and are in conversation with the US Department of Commerce to improve the Safe Harbour Agreement to ensure it plays its original role. In the meantime, cloud customers are losing trust in US-based providers and find that there are not many alternatives. They also find it evermore difficult to make sense of the reality of privacy risks and relevant regulation necessary for compliance. In response, the established, US-based vendors take action to increase transparency and local responsiveness, while European niche players emerge, largely encouraged by the European Union.

How exactly the landscape is going to turn out is still a question, but one thing seems to be sure: there is a trend towards more location-awareness regarding cloud computing. And just as Goldsmith and Wu (2006) earlier uncovered the illusion of the Internet creating a borderless world, we now learn that the black-boxed perception of a geography-independent cloud computing arena is just as an illusion.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Petterson, D., Rabkin, A., Stoica, I., and Zaharia, M. (2010) A view of cloud computing. *Communications of the ACM*, 53(4): 50.

Ball, J., Borger, J., Davies, N., Hopkings, N., MacAskill, E. (2013) GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian* Retrieved from: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-ns

Castro, D. (2013) How Much Will PRISM Cost the U.S. Cloud Computing Industry? *The Innovation Technology & Innovation Foundation*. Retrieved from: http://www2.itif.org/2013-cloud-computing-costs.pdf, accessed 12th July 2014

Clark, L., 2014. Europe need NSA-proof Internet, says Germany. *Wired*. Retrieved from: http://www.wired.co.uk/news/archive/2014-02/17/merkel-national-web, accessed 12th July 2014

Clarke, R. and Svantesson, D. (2010) Privacy and consumer risks in cloud computing. *Computer Law and Security Review*, 26(4): 391-397.

Cloud Security Alliance (2013a) Government Access to Information Survey Results. Retrieved from: https://cloudsecurityalliance.org/download/government-access-to-information-survey-results/, accessed 12th July 2014

Cloud Security Alliance (2013b) Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union. *Privacy Level Agreement Working Group*. Retrieved from: https://cloudsecurityalliance.org/download/privacy-level-agreement-pla-outline-for-the-sale-of-cloud-service-providers-providing-services-in-the-european-union/, accessed 12th July 2014

Corbin, K. (2014) Cloud Service Providers Fight Back, Challenge NSA. *CIO.com*. Retrieved from: http://www.cio.com/article/748791/Cloud_Service_Providers_Fight_Back_Challenge_NSA?page=1&taxonomyId=3133, accessed 12th July 2014

Darrow, B. (2012) Buckle up for a new wave of cloud protectionism. *Gigaom*. Retrieved from: http://gigaom.com/2012/01/17/buckle-up-for-a-new-wave-of-cloud-protectionism/, accessed 12th July 2014

European Commission (2012) *Digital Agenda: New strategy to drive European business and government productivity via cloud computing*. Retrieved from: http://europa.eu/rapid/press-release_IP-12-1025_en.htm, accessed 12th July 2014

European Commission (2013) *Memo: What does the Commission mean by Secure Cloud computing services in Europe?* Retrieved from: http://europa.eu/rapid/press-release_MEMO-13-898_en.htm, accessed 12th July 2014

European Parliament (2013) *Reports on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN, accessed 12th July 2014

Export.gov (n.d.) U.S.-EU SAFE HARBOR LIST Retrieved from: http://safeharbor.export.gov/list.aspx, accessed 14th July 2014

Galliers, R.D., Newell, S., and Swan, J.A. (2001) A knowledge-focused perspective on the diffusion and adoption of complex information technologies: the BPR example. *Information Systems Journal*, 10(3): 239-259.

Goldsmitsh, J. and Wu, T. (2006) Who controls the Internet? Illusions of a borderless world Oxford University Press

Google (2014) *Transparency Report*. Retrieved from: http://www.google.com/transparencyreport/userdatarequests/countries/, accessed 14th July 2014

Grance, T. and Jansen, W. (2011) Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication*. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf., accessed 14th July 2014

Greenwald, G. and MacAskill, E. (2013) NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed 14th July 2014

Grimes J.M., Jaeger, P.T., Linn, J. and Simmons, S.N. (2009) Where is the cloud? Geography, economics, environment, and jurisdiction

in cloud computing. *First Monday* 14(5): 1-16. Retrieved from: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171, accessed 14th July 2014

Hakim, D. (2013) Europe Aims to Regulate the Cloud. *The New York Times*. Retrieved from: http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html?pagewanted=all&_r=0, accessed 14th July 2014

IBM, 2014. *Press release: IBM Commits $1.2 Billion to Expand Global Cloud Footprint*. Retrieved from: http://www-03.ibm.com/press/us/en/pressrelease/42956.wss, accessed 14th July 2014

Juskalian, R. (2014) For Swiss Data Industry, NSA Leaks Are Good as Gold. *MIT Technology Review*. Available online at: http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/, accessed 14th July 2014

King N.J. and Raja V.T. (2013) What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. *American Business Law Journal*, 50(2): 413-482, accessed 14th July 2014

Larson, J., Perloth, N. and Shane, S. (2013) N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*. Retrieved from: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=1&, accessed 14th July 2014

Mell, P. (2009) Effectively and Securely Using the Cloud Computing Paradigm. Information Technology Laboratory. Retrieved from: http://www.secureit.com/resources/Cloud%20Computing%20Peter%20Mell%20NIST%205-09.pdf, accessed 14th July 2014

Miller, P. (2014) Sector RoadMap: the European cloud infrastructure market. *Gigaom*. Retrieved from: http://research.gigaom.com/report/sector-roadmap-the-european-cloud-infrastructure-market/, accessed 14th July 2014

Pearson, S. (2009) Taking Account of Privacy when Designing Cloud Computing Services. *ICSE'09 Workshop*, Vancouver, Canada. Retrieved from: http://www.hpl.hp.com/techreports/2009/HPL-2009-54.pdf, accessed 16th July 2014

Reding, V. (2014) Future of the Safe Harbour Agreement in the light of the NSA affair. European Commission. Retrieved from: http://europa.eu/rapid/press-release_SPEECH-14-27_en.htm, accessed 16th July 2014

Seiffert, J. (2014) Weighing a Schengen zone for Europe's Internet data Germany. *Deutsche Welle*. Retrieved from: http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482, accessed 16th July 2014

Swanson, E.B. and Ramiller, N.C. (1997) The Organizing Vision in Information Systems Innovation. *Organization Science*, 8(5): 458-474.

Tielmans, J. (2014) Dissuading Companies from Violating Data Protection Rules: Senior European Commission Official Calls for 'Significant' Fines. *Inside Privacy*. Retrieved from: http://www.insideprivacy.com/international/dissuading-companies-from-violating-data-protection-rules-senior-european-commission-official-calls/, accessed 16th July 2014

van der Meulen, R. and Rivera, J. (2013) *Press release: Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion* . Gartner. Retrieved from: http://www.gartner.com/newsroom/id/2352816, accessed 16th July 2014

Veld V. and van der Zwet, J.F. (n.d.) The Evolution Of The European Cloud Market. *interxion*. Retrieved from: http://www.interxion.com/sectors/cloud/hosting-providers/the-evolution-of-the-european-cloud-market/, accessed 16th July 2014.

Venters, W. and Whitley E.A. (2012) A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*, 27: 179–197

Willcocks, Leslie P. and Venters, Will and Whitley, Edgar A. (2012) Cloud and the Future of Business: from Cost to Innovation. Accenture. Retrieved from: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Cloud-Future-Business-Costs-Innovation-Part-Two-Challenges.pdf, accessed 16th July 2014.

Whitley, E.A. (2014a) Privacy and Security in the Cloud: A Review Of Guidance and Responses. *Journal of International Technology and Information Management* (in press)

Whittaker, Z. (2011a) How the USA PATRIOT Act can be used to access EU data. *ZDNet*. Retrieved from: http://www.zdnet.com/blog/igeneration/case-study-how-the-usa-patriot-act-can-be-used-to-access-eu-data/8805, accessed 16th July 2014.

Whittaker, Z. (2011b) Microsoft admits Patriot Act can access EU-based cloud data. *ZDNet*. Retrieved from: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225, accessed 16th July 2014.

Xiao, Z.F. and Xiao, Y. (2013) Security and Privacy in Cloud Computing. *Ieee Communications Surveys and Tutorials*, 15(2): 843-859.

Zorz, Z. (2013) FISAA legalizes surveillance of EU citizens and their cloud data, claims study. *cybersecurity.org*. Retrieved from: http://www.net-security.org/secworld.php?id=14215, accessed 16th July 2014.