Public Policy and Regulatory Implications for the Implementation of Opportunistic Cloud Computing Services for Enterprises

Eric Kuada, Henning Olesen and Anders Henten
Center for Communication, Media and Information Technologies, Aalborg University,
Sydhavnsgade 17, Copenhagen, Denmark

Abstract. Opportunistic Cloud Computing Services (OCCS) is a social network approach to the provisioning and management of cloud computing services for enterprises. This paper discusses how public policy and regulations will impact on OCCS implementation. We rely on documented publicly available government and corporate policies on the adoption of cloud computing services and deduce the impact of these policies on their adoption of opportunistic cloud computing services. We conclude that there are regulatory challenges on data protection that raises issues for cloud computing adoption in general; and the lack of a single globally accepted data protection standard poses some challenges for very successful implementation of OCCS for companies. However, the direction of current public and corporate policies on cloud computing make a good case for them to try out opportunistic cloud computing services.

1 Introduction

Chief Information Officers (CIOs) and Information Technology (IT) managers have over the past two decades successfully handled overseeing the convergence of voice and data networks to support the business process of their organisations. IT departments currently face the daunting task of ensuring compliance, data security and cutting down on operational cost amidst tight spending budgets. There is also a growing expectation from Chief Executive Officers (CEOs) and boards of directors for information technology's mission to quickly expand from cost cutting to revenue generation. Enabling revenue growth involves aligning IT strategy and capabilities with the overall business objectives mainly through knowledge management and supporting collaboration with partners.

As CIOs wake up to their new corporate mandate, they are seeking to tap organisational and technical solutions to improve IT's fit with business objectives which is also likely to involve the painful process of the decentralisation of IT departments authority and functions to other business units [15].

But for compliance and data security challenges which are generating serious policy and regulatory challenges for cloud computing adoption, it seems an excellent solution to the challenges that IT departments currently face. Cloud Computing [12],[11] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage,

Kuada E., Olesen H. and Henten A..
Public Policy and Regulatory Implications for the Implementation of Opportunistic Cloud Computing Services for Enterprises.
DOI: 10.5220/0004086300030013
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 3-13
ISBN: 978-989-8565-15-0

applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Perhaps the most paramount factor for the adoption of cloud computing by any organisation is that of cost reduction in the purchase and operation of IT solutions. It obviates the need for huge initial capital expenditure involved in the acquisition of IT infrastructure and solutions which are normally underutilised or may later not be suitable for their intended purpose; and allow for the payment for resources as per their actual usage. Cloud computing also offers the agility, scalability and elasticity that IT departments require in coping with changing business needs of the organisations that they serve. These factors together with the transformation of the roles of IT departments and their staff that cloud computing bring to organisations result in efficient IT service delivery.

Enabling revenue growth comes from the transformation of IT departments' roles, promoting business-to-business (B2B) integration with partners and creation of new business models. With the adoption of cloud computing services the role of IT departments must evolve from that of a service and support provider to that of certification and management of cloud services. As a result the roles of IT staff members also shift from task-oriented administrators of infrastructure and application services to that of strategic planners, project managers or business analysts who understands the company's business processes and end-user needs to support them better. The adoption of cloud computing by any two companies in general reduces the complexities involved in B2B integration. Companies can therefore leverage cloud computing by exposing their business processes to potentially large ecosystems of partners who often find ways of joining and integrating their business processes in the value chain.

Compliance risk management, security and privacy issues are however generating serious policy and regulatory challenges for cloud computing adoption. The introduction of the concept of Opportunistic Cloud Computing Services (OCCS) for enterprises will certainly not make these challenges any lighter. Because OCCS promises an accelerated adoption and further reduction in IT cost for small companies, we have been working on the feasibility of its successful implementation in terms of the technical feasibility, developing suitable incentive mechanisms to promote contribution of services to the platform, and its acceptance and support by all stakeholders. This paper discusses how public policy and regulations will impact on OCCS implementation. The rest of the paper is organised as follows: Section 2 gives an overview of cloud computing and the concept of opportunistic cloud computing services. Section 3 presents governments strategic policies towards cloud computing adoptions and the guiding regulations. Based on the results from Section 3, Section 4 discusses how these public and corporate strategies will impact on the implementation of OCCS. Section 5 concludes the paper and Section 6 touches on our future work.

2 Background

To put the subsequent sections in context, the first part of this section gives a brief overview of cloud computing in general and the second part briefly presents the

opportunistic cloud computing services concept and its motivation. Details about it and its reference architecture can be found in [9].

2.1 Overview of Cloud Computing

Cloud computing is essentially the packaging of traditional information technology infrastructure and software solutions such as storage, CPU, network, applications, services, etc. as virtualized resources and delivered by a service provider to its customers as an on-demand pay-per-use self-provisioned service through a web portal over a network such as the Internet. There have been major technological advancements as well as social and business demands driving this new trend of computing. The technological factors facilitating cloud computing include the availability and drastic increase in reliable broadband Internet access, advancements in virtualization technologies and the shift of development of majority of both desktop and enterprise applications as web services and applications.

The three main components of a regular computing environment, namely the hardware infrastructure, the operating system platform and user application software, have respectively translated into Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) delivered in cloud computing. Additionally, there is an inexhaustible list of other cloud computing services due to the concept of "Anything as a Service" (XaaS) being the main driving idea of cloud computing. Thus, virtually all IT products and solutions are potential cloud computing services. These services are normally deployed in four main cloud deployment models namely public, private, community, and hybrid cloud computing deployment models [7].

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud service provider selling cloud services and by definition, is external to an organization. At the other end of the spectrum are private clouds. A private cloud is one in which the computing environment is operated exclusively for an organization; a private cloud may be managed either by the organization itself or a third party such as a commercial cloud services provider, and may be hosted within the organization's data centre or outside of it. The community clouds and hybrid clouds fall between public and private cloud deployment models. A community cloud is somewhat similar to a private cloud, but the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization. A hybrid cloud deployment model is a combination of two or more of the other cloud models (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technologies that enable interoperability.

2.2 Overview of Opportunistic Cloud Computing Services

Opportunistic cloud computing service is a social network approach to the provisioning and management of cloud computing services for enterprises [9]. OCCS deals with the concept of enterprises taking advantage of cloud computing services to

meet their business needs without having to pay or paying a minimal fee for the services. The OCCS network is a social network of enterprises collaborating strategically (possibly selfishly) for the contribution and usage of cloud computing services without entering into any business agreements. Unlike social networking services provide by social networking sites for individual use where users create their own network of friends, in an OCCS network, members do not explicitly create ties with other members but these ties come indirectly through the services and resource contribution and consumption process.

The OCCS network platform is a governing platform that serves as the social networking platform for enterprises and also includes interoperable Cloud management tools with which member enterprises can provision cloud computing services that would be used by other enterprises interested in these services. The OCCS platform thus consists of two main layers – the service layer and the management layer. The service layer consists of all the services contributed by members. These will normally be fundamental cloud computing services such as SaaS, PaaS, and IaaS; but, it can also include value added services normally provided by cloud service brokers. The management layer consists of two main components – the governance component that manages the services from members and cloud services brokerage (CSB) component that serves as an interface between the OCCS network and commercial cloud services providers and cloud service brokers.

The motivation for the OCCS concept is that there are underutilized spare resources available at some companies or organisations that can be useful to others that need them. Additionally the data centre and Cloud management competences that companies develop over time through managing their own resources can be of value to others lacking such competences (e.g. SMEs needs, especially in the developing world). OCCS also has the potential of fostering business collaborations, offering further reduction of cost in IT services and by design is compatible with future cloud computing technologies and solutions. There are currently policy and regulatory challenges for cloud computing and OCCS implementation may bring its unique challenges to these policies and regulations.

3 Policy and Regulatory Issues of Cloud Computing

This section presents the various strategic policies being adopted in North America, Europe, Asia Pacific and Africa. Representative countries in these regional blocks with documented publicly available government cloud computing strategic policies are presented and their policies taken as representative for that region. This approach of looking at things from a global perspective has been adopted instead of just at the national level because OCCS needs international scope to flourish. The implementation of national OCCS networks is useful; however, for participating members to find suitable services to meet their business needs, then the broader the scope of the platform the better. The section ends with a summary of the salient overriding goals driving these strategies and the main regulatory environments guiding them as is evident from these strategic policies.

3.1 North American Policy

The United States of America government has instituted a "Cloud First" policy to harness the benefits of cloud computing. This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments [10]. Since Cloud computing can offer benefits in the cost, performance, and delivery of IT services to Federal agencies, the United States Department of Commerce anticipates that the use of Cloud Computing services will grow significantly over the next several years [16]. Cloud computing promises to have far-reaching effects on the systems and networks of federal agencies and other organizations, many of the features that make cloud computing attractive, however, can also be at odds with traditional security models and controls. The policy is therefore to guide federal departments and agencies to carefully plan their Cloud initiatives to meet the organizational and national security and privacy requirements [7].

The Canadian government cloud strategy is in two folds. The first is to position itself as a world leader in cloud computing and the second is its cloud first policy being modeled after that of United States. Due to its geographical characteristics, low-density population, IT expertise, quality construction standards, legislative framework (including the Privacy Act and the Personal Information Protection and Electronic Documents Act) and low-cost green energy, Canada considers itself a prime location for cloud computing. Government of Canada and the provinces and territories are beginning to realize Canada's advantage and the benefits of positioning Canada as an economical and strategic choice for cloud computing [4].

3.2 European Union Policy

The European Union is in the process of finalizing the EU Cloud computing strategy and is yet to publish a formal document on it. The approach of leading EU member nations like Germany and France had suggested home grown national Clouds or at best an Europe first cloud policy mainly in response to the US Patriot Act; but recommendations towards the European Commission's call for contributions to an EU strategy on Cloud Computing seems to suggest otherwise. DIGITALEUROPE urges the EU to let the EU cloud computing strategy transcend national and regional borders and rather play a leadership role in negotiating global collaboration in addressing jurisdiction and clarifying rules on law enforcements access to data stored in the Cloud; and adopt or implement policies that address actual or potential trade barriers to the evolution of cloud computing [5].

The United Kingdom government has decided to opt for a combination of private and public cloud through its G-Cloud programme after weighing the benefits of both. The Government cloud is not a single, government owned, entity; it is an on-going and iterative programme of work which will enable the use of a range of cloud services and make changes in the way it procure and operate ICT services and solutions throughout the public sector. The vision is for the government to robustly adopt a public cloud first policy; this however will not be possible in every case and there will also be a requirement for a private G-Cloud. The government will push

ahead with its agenda for data centre, network, software and asset consolidation and the shift towards cloud computing. It will mandate the reuse of proven, common application solutions and policies. These solutions must balance the need to be open, accessible and usable with the growing cyber-security threat and the need to handle sensitive information with due care [2]. This will be achieved through three main projects - Data Centre Consolidation, the G-Cloud, and the Applications Store for Government. The overriding goals are reduce ICT costs, provide open competition and create a vibrant marketplace enabling the best product at the best price, create flexibility by reducing supplier lock-in to ensure users can readily switch between suppliers for ICT services, reduce time from idea to service, and reduce the carbon footprint of Public Sector ICT services [14].

3.3 Asia Pacific Policy

According to a study by Frost & Sullivan in 2010 on the Asia Pacific region, 21 percent of respondents in the government sector have adopted cloud computing in one form or the other. Furthermore, it also revealed that given the governments concerns around security of data and location of data centres, private and hybrid clouds are witnessing significantly higher adoption in the region [3]. Though countries in the region are at different stages of forming a cloud strategy their current initiatives give an indication of their cloud policies to be adopted.

Some of these initiatives are: despite the quite circumspective approach the Australian Government has taken in adopting cloud computing primarily due to their uncertainty over storing data in offshore data centres, given the shrinking ICT budgets certain agencies have gone ahead to try out cloud computing services. The Chinese government besides other projects through its “cloud factory” project is providing adequate computing resources to enterprises which are mainly start-ups without the financial power to acquire the required IT assets. Other countries in the region have similar policies centred on cost reduction, green IT, developing local expertise, research on cloud services, providing subsidies to enterprises to boost industry participation, and perhaps most importantly building national private clouds due to concerns of data security and jurisdiction of location of data centres.

3.4 African Policy

The African cloud computing strategic policy as of now seems to be “no policy” and there is no direct effort from governments to create one. The closest documented action towards a cloud computing policy for Africa is an ITU organized forum held in Rwanda which came up with two main recommendations towards a cloud computing strategy for Africa. The first is physical interconnections between African countries via broadband networks are a prerequisite for successful implementation of cloud computing applications and systems. African States must take the necessary action to develop broadband in Africa, improve national, regional and international connectivity. The second is that in order to take advantage of the opportunities afforded by cloud computing while minimizing risks, African States must have a coordinated and coherent approach to their adoption of cloud computing and

transition to it. In that regard, they must adopt guidelines on the strategy for the transition to cloud computing, capacity-building programmes, the harmonization of legislative and regulatory reference frames, the adoption of data centre selection criteria, and attracting investment and seizing business opportunities [6].

Cost reduction and efficiency in the delivery of IT services is a central motivation in all the policies discussed above; on the other hand meeting security and privacy requirements for the protection of both national and citizen data are major issues that the policies try to address. It is however also evident that the national and regional strategies being adopted are dependent on the economic environment, their current ICT policy, data protection laws and current infrastructure; the different regions are therefore at different levels of the evaluation and deployment of cloud computing services. For example because the major cloud services vendors and providers are of USA origins coupled with the Patriot Act that compels these companies to release information or data stored on the service providers platforms to their law enforcement agencies irrespective of location where the data is stored makes the USA a little more open to public cloud services than the rest of the world, particularly Europe which has tighter regulations of the protection of privacy of citizen data.

4 Impacts of Policy and Regulations on OCCS

Governments' adoption of commercial cloud services reduces potential resources that would have been made available to OCCS. With the current state of highly underutilized resources in government data centres, these would have been perfect resources to have been contributed to the OCCS platform. However, with the governments already adopting commercial cloud computing services these spare resources diminish. A major part of government cloud computing services adoption is in building their private clouds. This has been necessitated by fears of commercial cloud services providers not meeting the security requirements for national information and privacy of citizen data. Even when commercial cloud services providers have been contracted to provide these cloud computing services, governments have insisted that the services be hosted within the borders of their own country.

It is evident from this that most cloud service needs by the public sector of most governments cannot generally be provided by an OCCS network with international scope. Even for those public sector applications that are found to be suitable for utilizing OCCS resources, the OCCS platform will have to provide commercial grade reliability, security and privacy guarantees for it to be useful for government public sector consumption of these services.

The national and regional strategies with focus on investing in cloud computing services to support start-up companies in meeting their IT resources requirements and the promotion of industry participation through subsidies will find OCCS a very useful approach to take. Instead of a direct government investment in providing cloud computing services to these companies, a conducive environment can rather be created for other companies to provide such resources. Government strategies on the promotion of Digital Business Ecosystems, and development of local expertise in cloud computing will also find OCCS a very useful approach. National OCCS

networks can be created whereby such cloud computing management competences are developed through the provisioning of cloud services to other companies. The resulting OCCS business ecosystems will also catalyse business growth through new start-up companies and fostering business collaborations.

The promotion of OCCS implementation inherently resolves cloud computing standards, interoperability and vendor lock-in issues. The current cloud computing industry is still dominated by proprietary technologies from the leading cloud service vendors and cloud management tool developers. This makes interoperability a serious issue defeating the purpose of flexibility and freedom of choice that cloud computing is supposed to provide to users and thereby resulting in vendor lock-in that users have to grapple with when it becomes necessary to change their cloud service provider. As has been indicated by [9] a successful implementation of an OCCS network must provide support for the management of fundamental cloud computing services, support for the management of any arbitrary cloud computing service, interoperability with major cloud computing standards and cloud computing management tools, and support for future cloud management technologies. Thus to start with, the OCCS concept must carefully follow cloud computing standards; the situation is however reversed as OCCS network implementations become successful. Thus those standards that are dominant on the OCCS platform will then be followed closely by cloud management tool developers and cloud service providers. This will further promote the success of the OCCS platform; and hence the promotion of cloud computing standardization and promotion of the OCCS implementations will be in a virtuous cycle.

The move by companies to the adoption of cloud computing is a senior management level (the CIO, Head of IT or IT Director) driven strategic technology shift for organizations as they look to lower costs and evolve their computing models to deliver competitive advantage to their businesses. The majority of 46 percent in an AMD sponsored research in 2011 on the adoption trends of cloud computing stated it was a strategic shift in IT policy for the organization with just 19 percent describing it as a cost-saving necessity, and with 35 percent stating it is a tactical move to address a specific need [13]. It is however important to note that even though less than a fifth find it a cost-saving necessity, cost reduction has been a factor in all cases. The further reduction of cost in IT services that OCCS provides is attractive to companies - especially very small companies which normally have lower demands on reliability and with a tighter IT budget.

4.1 Regulatory Amendments to Support OCCS

OCCS needs international scope to flourish. The implementation of national OCCS networks is useful; however, for participating members to find suitable services to meet their business needs, then the larger the scope of the platform the better. Secondly users should be indifferent (should not need to worry) about the location or origins of the provider of the service in which they are interested in utilizing. It should also be noted that no SLAs exist between the provider of a service and possible user of that service on the OCCS platform. And the rules of conduct governing the platform should not put undue burden on contributors of resources and services to the platform.

Currently US companies need to use the US-European Union and the US-Switzerland Safe Harbour Frameworks to meet European "adequacy" standards for privacy protection [1]. The recently proposed EU data protection reform [17] which is meant to be cloud computing friendly proposed a "Regulation to replace a Directive: that means a single set of rules for Europe, not 27 different ones. Alongside that, under the new rules you will get a one-stop-shop of enforcement; so that, even if an operator is active in several EU countries, it will only have to deal with one data protection authority – the one where its main base is. Cloud users should not have to guess where their provider is: if a company offers goods or services to people in the EU, or is monitoring them, then it shouldn't matter where that company's based – in Madrid, Mumbai or Mountain View. Our rules should apply to the data" [8]. The proposed regulations are expected to make it easier to operate Clouds within and outside the European single market.

Allowing Cloud operations to easily cross borders is a step in the right direction for both cloud computing in general and OCCS. It is not too much of a problem for commercial cloud service providers to go through the necessary trouble of meeting multiple data protection rules; however OCCS should not have to grapple with the "our rules apply" in the formulation of the rules on terms of conduct on the platform since it will be a very daunting task to formulate such rules without putting undue burden on contributors of services to the platform and simultaneously ensuring that participating enterprises on the platform are able to use such free resources in providing services to their customers that meet different national or regional rules on data privacy. Having a single set of globally accepted rules that govern data protection for Cloud operations will therefore be very beneficial for OCCS even though that would not be a sufficient condition for OCCS to be very successful.

5 Conclusions

The paper has discussed the impact that public policy and current regulations together with corporate strategies towards cloud computing adoption will have on the implementation of opportunistic cloud computing services. We have looked at the various strategic policies being adopted by North America, Europe, Asia Pacific and Africa. Cost reduction and efficiency in the delivery of IT services is a central motivation in all the policies; on the other hand meeting security and privacy requirements for the protection of both national and citizen data are major issues that the policies try to address. The move by companies to the adoption of cloud computing is a senior management level driven strategic technology shift for organizations as they look to lower costs and evolve their computing models to deliver competitive advantage to their businesses. The further reduction of cost in IT services that OCCS provides is attractive to companies - especially very small companies which normally have lower demands on reliability and with a tighter IT budget.

We conclude that there are regulatory challenges on data protection that raises issues for cloud computing adoption in general; and the lack of a single globally accepted data protection standard poses some challenges for very successful implementation of OCCS for companies. However, the direction of current public and

corporate policies on cloud computing make a good case for them to try out opportunistic cloud computing services.

6 Future Work

This work has relied on documented publicly available government and corporate policies on the adoption of cloud computing service and has deduced the impact of these policies on the implementation and adoption of opportunistic cloud computing services. Our future work will include results from interviews that will be conducted on representative organisations of the various sectors of the economy. Secondly based one of the findings of this work that the OCCS platform will have to provide commercial grade reliability, security and privacy guarantees for it to be useful for government public sector consumption of these services, we will also work on trust and security frameworks and their implementations for OCCS.

References

1. U.S. Department of Commerce, 2012. Safe Harbor. [Online] Available at: http://export.gov/safeharbor/index.asp [Accessed 29 04 2012].
2. Cabinet Office, 2011. Government Cloud Strategy, London SW1A 1AS: Crown.
3. Chandrasekaran, A. & Kapoor, M., 2011. State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific, s.l.: Frost & Sullivan.
4. Danek, J., 2009. Cloud Computing and the Canadian Environment, Ottawa, Ontario: s.n.
5. DIGITALEUROPE, 2011. Cloud Computing, DIGITALEUROPE'S PERSPECTIVE, Brussels: s.n.
6. ITU FTRA-2011, 2011. Cloud computing, development prospects of ICTs: Challenges and opportunities for the policymakers, regulators and ICT operators. [Online] [Accessed 8th March 2012].
7. Jansen, W. & Grance, T., 2011. Guidelines on Security and Privacy in Public Cloud Computing, Gaithersburg: National Institute of Standards and Technology.
8. Kroes, N., 2012. EU Data protection reform and Cloud Computing. [Online] Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en [Accessed 30 April 2012].
9. Kuada, E. & Olesen, H., 2011. A Social Network Approach to Provisioning and Management of Cloud Computing Services for Enterprises. Rome, Italy, Sep.2011, CLOUD COMPUTING 2011 : The Second International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 98 - 104.
10. Kundra, V., 2011. Federal Cloud Computing Strategy, Washington DC: s.n.
11. Marston, Sean; et al;, 2010. Cloud computing - the business perspective. ELSEVIER, December.Volume Decision Support Systems.
12. Mell, P. & Grance, T., 2009. The NIST Definition of Cloud Computing, USA: s.n.
13. Red Shift Research, 2011. Adoption, Approaches & Attitudes, The Future of Cloud Computing in the Public and Private Sectors, s.l.: AMD.
14. Tait, A., 2010. G-Cloud Founding Principles, London: Cabinet Office.
15. The Economist Intelligence Unit , 2006. Great expectations: The changing role of IT in the business, London: The Economist.

16. U.S. Department of Commerce, 2010. Cloud Computing Policy. [Online] [Accessed 1 March 2012].
17. Viviane Reding, EU Justice Commissioner, 2012. Data protection reform: Frequently asked questions. [Online] Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=en [Accessed 30 April 2012].