THE IMPACT OF EXISTING SOUTH AFRICAN ICT POLICIES AND REGULATORY LAWS ON CLOUD COMPUTING: A LITERATURE REVIEW

Mpho Mohlameane[1] and Nkqubela Ruxwana[2]

[1]The Da Vinci Institute, 16 Park Avenue, Modderfontein, South Africa
mpho.mohlameane@gmail.com
[2]Tshwane University of Technology, 2 Aubrey Matlakala St,
Soshanguve, Pretorita, South Africa
ruxwananl@tut.ac.za

ABSTRACT

Cloud computing promises good opportunities for economies around the world, as it can help reduce capital expenditure and administration costs, and improve resource utilization. However there are challenges regarding the adoption of cloud computing, key amongst those are security and privacy, reliability and liability, access and usage restriction. Some of these challenges lead to a need for cloud computing policy so that they can be addressed. The purpose of this paper is twofold. First is to discuss challenges that prompt a need for cloud computing policy. Secondly, is to look at South African ICT policies and regulatory laws in relation to the emergence of cloud computing.

Since this is literature review paper, the data was collected mainly through literature reviews. The findings reveals that indeed cloud computing raises policy challenges that needs to be addressed by policy makers. A lack of policy that addresses cloud computing challenges can negatively have an impact on areas such as security and privacy, competition, intellectual property and liability, consumer protection, cross border and juridical challenges.

KEYWORDS

Cloud Computing, Policy, Law, Regulation.

1. INTRODUCTION

Technology evolution has helped economies around the world to become more competitive. The emergence of Information and Communication technology (ICT) has helped businesses around the world to streamline and improve their business processes in order to respond quickly to customer needs. Of those technology evolution, cloud computing happens to be a technology that when used, it can help reduces capital expenditure and furthermore improve competitiveness globally.

David C. Wyld et al. (Eds) : ICAITA, CDKP, CMC, SOFT, SAI - 2016
pp. 11– 24, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61302

However, with technology evolution such as cloud computing, there are some noticeable challenges which might hinder the adoption rate and therefore deny companies economy of scale. Key amongst those challenges includes security and privacy, reliability and liability, access and usage restriction. Therefore such challenges necessitate a need for cloud computing policy that when adopted, it can help improve public confidence in the adoption and use of cloud computing and furthermore help improve competitiveness.

In this paper we set the scene by first describing the overview of cloud computing, more specifically defining cloud computing and also a brief discussion of cloud deployment models and services. We then proceed by discussing key challenges that leads to a need for cloud computing policy. We furthermore move to the core aspect of this paper which is the discussion of key South African laws and regulation in relation to cloud computing.

The next section describe the overview of cloud computing, starting with the definition of cloud.

2. OVERVIEW OF CLOUD COMPUTING

2.1. Definition of Cloud computing

Cloud computing can be briefly defined as computing over the internet, whereby services such as data storage, application software are accessible over the internet [1]. The European Community for Software and Services [2] defines cloud computing as "the delivery of computational resources from a location other than your current one"

The National Institute of Standard and Technology (NIST) gave a detailed definition as they define cloud computing as " a model for enabling 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" [3].

The above definitions characterise cloud computing as convenient and on-demand service, shared resource pooling, rapid elasticity and broad network access [12].

2.2. Cloud Computing Deployment Models

By cloud deployment models, we refer to cloud targeted deployment models such as public, private, hybrid and community.

- **Public Cloud** – refers to computing services that are publicly accessible over the internet by subscribed cloud consumers. Examples of public cloud services includes but not limited to Google Email, Google Drive, Dropbox, Amazon Web Services (AWS), etc. [4] [5].

- **Private Clouds** – unlike public clouds whereby the hosting infrastructure and software application is hosted by third party and there is multi-tenancy of different cloud customers, private clouds are privately owned and accessible privately. In most cases enterprises that have deployed private clouds choose not to publish some of the private and confidential data to public cloud, rather manage such sensitive data internally [4] [5].

- **Hybrid Clouds** – is made up of two or more clouds with the characteristics of both private and public cloud [7], [8], [9]. NIST [3] corroborates the above by defining hybrid cloud as "a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

- **Community Cloud** – Institutions with shared mission and goals, computing needs, policies and security requirements can form what is termed "community cloud" as a means to share hosting infrastructure (hardware, network resources, etc.) amongst community members [4], [5], [10].

2.3. Cloud Computing Service Models

Cloud services models refers to computing services that are offered on the cloud. These includes services such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) [11].

- **Platform as a Service** are services that creates a platform for software application developers to develop, deploy and manage their applications over the internet. Examples of PaaS include but no limited to Amazon Elastic Beanstalk, Microsoft Windows Azure, Google App Engine, and Apache Stratos.

- **Infrastructure as a Service** are services that provides customers with hardware and computing infrastructure that is typically hosted and managed by cloud computing service provider [13]. Examples includes but not limited to Amazon EC2, Google Compute Engine and Rackspace.

Software as a Service is the delivery of software solutions in a form of a service whereby the software is hosted by the service provider and is accessible over the internet. You don't necessary have to install the software locally on your computing device, rather you access it over the internet. The advantage therefore is the licensing model which is subscription based [16]. Examples includes Microsoft 365 office, Google Apps and Salesforce.

3. CHALLENGES THAT LEAD TO A NEED FOR CLOUD COMPUTING POLICY

There are several challenges that lead to a need for cloud computing policy that when addressed, can help improve public confidence and improve the adoption rate. These challenges are discussed below starting with key security and privacy.

3.1. Security and Data Privacy

Cloud services are accessible over the internet and are made up of cloud services such as email services (Gmail, Yahoo mail, etc.), social network (such as Facebook, etc.), storage services such as Dropbox, Google Drive, VMware storage services, etc. These cloud services stores huge

amount of personal and sensitive information at data centers around the world. Due to the fact that these data is accessible over the internet, this raises privacy and security risks.

Cloud computing like other networked systems, is more prone to traditional threats such as data confidentiality, privacy and authentication. This is because cloud computing resources are accessed over the internet and can be exposed to such security threats. Other threats includes but no limited to – abuse and nefarious use, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account and service hijacking.

Conversely, there are security issues which are more specific to the cloud environment and which are exacerbated by the multi-tenancy and distributed nature of the cloud. These include confidentiality, service availability, access control, identity management and privacy amongst the list [14], [15].

3.2. Access to the Cloud and Necessary ICT Infrastructure

Cloud computing due to its cost model, has the potential of enabling Small and Medium Enterprises (SMEs) to have access to the latest software services that will enable them to compete with large enterprises. Conversely, most of non-profit organisations make use of technological tools to advance their social and community developmental course. Since such organisations survive on donor funding, it makes sense to create access points to cloud services at a reduced cost.

Furthermore many countries have broadband challenges as most of it is not strong enough to enable business and general public to make use of cloud computing services, especially in rural places. Moreover, the cost of internet access and data usage tend to be expensive in most of countries, especially in South Africa.

3.3. Competition and Antitrust

The International Telecommunication Union (ITU) attributes the following as cloud computing competition concerns, namely: - data portability, lack of industry standards, public procurement practices and restrictive license condition [16]. Cloud computing deployment models consist of Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (Pass). ITU assert that “vendor lock-in” can occur within any of these three segments and this can become an impediment regarding data or application movements [16].

Conversely, Sluijs, Larouche and Sauter [17] identified three potential concerns which may constitute anticompetitive behaviour, namely 1) Interoperability and portability concerns, 2) Vertical integration and discrimination and 3) Internalization of market by a group of Internet Service Providers (ISP) to deny cloud computing providers to provide ubiquitous services. Vertical integration and discrimination could occur if the ISP decides to vertically integrate within the cloud computing market, i.e. deciding to provide cloud computing services as part of their differentiation strategy [17].

3.4. Wiretapping and Electronic Surveillance

In 2013, there were revelations made by former United States of Americas National Security Agency (NSA) contractor Edward Snowden regarding the NSA's programs that compromises the privacy of data stored in the cloud, especially the data that stored by USA cloud computing providers such as Microsoft and Google. The revelations by former NSA contractor has sparked public outrage in the cloud computing community. Such public outrage can negatively affect USA cloud providers doing business in other countries. This necessitate a need for transparency in electronic surveillance activities conducted by government agencies in order to ensure that the privacy of citizen is not violated.

3.5. Intellectual Property and Liability

As with on premise software, cloud computing services providers also rely on copyrights and patent laws and other forms of protections for their intellectual property (IP). We have recently witnessed companies such as Apple, Google and Microsoft filling patent and IP court papers seeking recourse due to the violation of their IP. Therefore to promote the development of cloud computing, there is a need for strong policy initiative that will comprehensively address issues of IP and copyright in order to protect cloud computing companies against any infringement of their IP and copyrights.

3.6. Consumer Protection and Vendor Lock-in

Issues of cloud reliability and liability necessitate a need for cloud computing policy regime. Cloud users expect cloud services to be reliable at all time, however this becomes a challenge. For instance cloud provider blackouts can render some of the mission critical applications unavailable.

Van Belle & Hinde [18] argues that Cloud computing risks and challenges from a South African perspective also include cloud lock-in. Cloud/Vendor lock–in is largely used by cloud vendors to technically ensure that consumers heavily depend on cloud vendor services, thus making it difficult for the consumer to easily switch from one vendor to another. Therefore there is a need to mitigate this cloud lock-in in order to ensure that consumers are protected from this and can easily switch from one vendor to another.

3.7. Cybercrime

The cloud computing market is growing rapidly and there is huge amount of data that is being stored on the cloud, and these vaults of data attracts cybercriminals. As cloud computing market grows, it will be very challenging to protect such data from cyber-attacks. This necessitate a need for a policy that will ensure effective law enforcement to deal with such acts of crimes.

3.8. Cross Border and Jurisdictional Challenges

Most cloud computing vendors have data centers around the world and most cloud consumers do not know the location where their information is stored. For instance, a cloud user staying in Nigeria can access his/her data that is stored in Australia. A question worth asking is which laws and regulations apply? The location of cloud provider's data center can have an influence the way

in which users are legally protected. There is a need for policy initiative that will address cross border cloud computing regulatory issues and therefore improve public confidence.

4. SOUTH AFRICAN POLICIES IN RELATION TO CLOUD COMPUTING: ANALYSIS AND DISCUSSION

The recent BSA Global Cloud Computing Scorecard survey done by the Software Alliance [19] revealed a significant improvement of South Africa regarding privacy laws and regulations. This is due to the recent privacy laws such as Protection of Personal Information Act (POPI). While cloud computing is gradually gaining its maturity and the usage increases, new challenges will eventually start to emerge.

For the purpose of this paper, three key regulatory laws are reviewed and discussed, namely POPI, Electronic Communication and Transaction Act, as well as The South African Competition Act. We purposefully selected these three regulatory laws as they are more inclined to the fundamental purpose of this study, as well as to analyse, discuss and interpret under the auspices of the identified challenges that leads to cloud computing policy, which were discussed in the previous section of this paper. Of those identified regulatory laws and regulations, we first start discussing and analysing POPI Act

4.1. Protection of Personal Information Act (POPI)

With the increase of criminal acts such as identity theft and the intrusion of personal privacy, governments all over the world have increasingly become concerned regarding these criminal acts as well as the way in which personal information is collected, handled and processed by companies. South Africa is not an exception to these global concerns of privacy issues, hence there is now a new act called the Protection of Personal Information Act (POPI) which was enacted on 26 November 2013.

The premise of POPI is to regulate the way in which organisations collect and process personal information for business purpose. This is done with the aim of ensuring that individual right to privacy is safeguarded. Therefore gone are the days whereby organisations could obtain individual personal information and process it without the consent of the data subject. The data subject is described as the person to whom the personal information relates [20]. POPI scope is very wide as it applies to almost every activity that one might do with the personal information, including the handling and processing of employees personal information.

The purpose of POPI is to uphold and enhance privacy of personal information as well as prescribing to international standards with regard to data privacy and protection [21]. POPI is influenced by other privacy regulations in countries such as the United Kingdom (UK), Canada, Australia and the European Union [21]. POPI act consists of 8 conditions regarding the lawful processing of personal information act, namely - accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject specification. These 8 principles are discussed below, starting with accountability condition.

Some of the advantages that can be drawn from the POPI Act is that it strives to ensure privacy, safety and confidentiality of data subject personal information. It strives to ensure that data is

processed in a lawful manner and with accountability. Furthermore, it ensures that the data subject participates in the process of processing of personal information. Moreover, it hold the responsible party and the operator accountable with regard to the unlawful processing of personal information. However it is worth mentioning that there are some noticeable challenges regarding POPI act.

POPI act is one of the comprehensive legislation act and compliance by companies is going to be a cumbersome process. The act allows companies to have in place privacy and security policies, however most of the enterprises do not have such policies [21], [22]. According to the survey conducted by ITWeb/Delloite, over 55% of companies participated in the survey did not have security or privacy policies in place [22]. Thus a lack of readiness in ensuring POPI compliance remains a concerns.

Furthermore, there are challenges with chapter 9 of the act which deals with cross-border data transfer. As discussed above, the act allows data to be transferred to other countries provided the data subject gives a concern and the laws and of the foreign country regarding privacy policies are similar to that of the republic. By having a restriction on information flow can affect international trade. From economic point of view, the unrestricted flow of information can ensure the development of global supply chain. While the restriction of information flow from privacy and security point of view makes sense, this has to be minimized to a level that it does not negatively impact global trade.

Another argument the researcher would like to raise regarding restrictive cross-border information flow is that in relation to competition. Most multinational companies like Google, Amazon and Microsoft offers competitive prices for their cloud computing services. Some of these multinationals stores personal information of data subject to countries which might not have privacy laws similar to that of South Africa, and as a result, this might have a competitive disadvantage for their South African market segment.

For instance, you might end up in a situation whereby there are local CSP which has local data centers but charges exorbitant prices compared to multinationals, because they comply with the act. It would be beneficial to maintain a balance between the POPI act and competitiveness, in order to ensure that there is economic growth through competitiveness and furthermore there is privacy laws that do not hinder such competitiveness and economic growth.

4.2. Electronic Communication and Transaction Act (ECTA 2002)

The Electronic Communication and Transaction Act (ETCA) was promulgated in 2002 in order to provide a regulatory framework to address electronic communications and other transactions conducted on the internet. With the increase of internet usage and e-commerce industry in South Africa, the ECTA was purposefully designed and implemented to:

- Facilitate and regulate the use of electronic communications and transactions.
- Necessitate the development of South African national e-strategy by the ministry of communication

- Promote access and use of electronic communication and transaction by Small, Micro and Medium Enterprises (SMMEs).

- Provide a regulatory framework to guard against abuse and malicious use of information systems.

- Promote the use of e-government services.

The ECTA of 2002 is a detailed regulatory act and consist of fourteen chapters outlining the government regulatory position regarding the use of electronic communication and online transaction. Furthermore the act address key factors such as and not limited to - facilitating electronic transactions, registration of cryptography providers, accreditation of authentication services providers, consumer and personal information protection in relation to electronic communication and transaction, liability of service providers and cybercrime.

One of the advantages of ECTA of 2002 is that some of the provisions in the Act are in line with international standards [23]. Another advantage of this Act is the provision for the protection of South African (SA) consumers, even though some critics suggest that the Act does so extensively to a level that it can create some trade challenges with international suppliers doing business with SA consumers [24].

The Act affords consumers with cooling-off period, to cancel without reason and penalty any credit agreement for the supply of goods within 7 days after the date of receipt of goods or services and within 7 days after the conclusion of the agreement. Therefore this serves as an advantage to the consumer as it afford him/her the opportunity to terminate the contract if he/she is not satisfied with the goods or services provided.

Cybercrime has become a global problem and the issue of cybercrime is not only affecting South Africa but other African countries as well [25];[26]. The increase in cybercrime in some countries in Africa is exacerbated by a rapid increase in the use of Information and communication technologies such smartphones, increased bandwidth, adoption of mobile money applications, etc. [27]; [28]; Kritzinger & von Solms, 2012). However the provision of cybercrime in the ACTA of 2002 serves as an advantage as it aims to address issues of cybercrime as well as making proclaiming cybercrime as a criminal offence punishable by jail term or fine.

There are notable challenges regarding this ECTA of 2002. De Villers [23] argued that some terms in the act are not clear, therefore there is a need for clarification of terms in order to increase legal certainty. Another challenge with this act is issues around trans-border jurisdiction and enforcement of judgment [23]; [29]. For instance, a South African consumer cannot institute a legal action against a supplier in a foreign country as the foreign court might refuse to recognize or enforce the ECTA of 2002.

Furthermore another challenges is around the use of cryptography as a form of data security, however with the emergence of cloud computing, the question is whether cryptography is compatible and sufficient enough in ensuring security online, the safety, integrity and authenticity of the data processed in the cloud environment. There seems to be are security challenges regarding the use of cryptographic in the cloud environment [30]; [31];[32]. Due to the diverse

layers of cloud computing, it is complex to manage cryptographic keys. Van Dijk and Juels [33] argued that the use of cryptography alone in enforcing privacy is not sufficient enough.

Another challenge with this act is that it was promulgated a decade ago and there are concerns regarding its applicability with the advancement of technology [34], such as cloud computing, mobile commerce, smartphones, phablets, and so forth. The advancement in technology necessitate a need for policy makers to review and adjust policies. Failure to do this will render some policies inefficient and raise gaps which can then cause problems.

4.3. The South African Competition Act

The South African government has a competition policy which was drafted in the early years of our democracy. The then new administration of the founding father of our democracy, the late Tata Nelson Mandela, brought new policy reforms. Tata is isiXhosa word that means "Father" and it is this word that many South Africans use to refer to the late President Nelson Mandela.
The policy reforms back then were necessary as part of a country's comprehensive program for economic, social and political transformation and as well as the re-integration of South African economy in a global economy after years of exclusion and isolation under the apartheid regime [35]. In October 1998, the South African competition act was legislated and became an act regulating competition in South Africa. The purpose of the South African competition act is to promote and sustain completion in South Africa, by:

- *The promotion of the efficiency, adaptability and development of the economy.*
- *Providing consumers with competitive prices and product choices.*
- *The promotion of employment and the advancement of the social and economic welfare of South Africans.*
- *The expansion of opportunities for South African participation in world markets and recognizing the role of foreign competition in the Republic.*
- *Ensuring that small and medium-sized enterprises have an equitable opportunity to participate in the economy.*
- *The promotion of a greater spread of ownership, in particular to increase the ownership stakes of historically disadvantaged persons.*[36]

From the objectives above, it can be argued that the aim of South African competition act is twofold or rather has a dual objective [37], firstly to promote and sustain competition in South African, and secondly to achieve economic transformation in South Africa and address "the historical economic structure and encourage broad-based economic growth" [38].

One of the advantages of the South African Competition Act is the control of anti-competitive conduct and the promotion of competition within the domestic market [40]. Due to the fact that South African emerged from a highly segregated society and with the economy used to be dominated by large conglomerates [40], it was therefore necessary to design a policy that is inclusive and promotes fair competition. The promotion of competition within the domestic

market includes the participation of previously disadvantaged people (mainly African natives) so that they can also participate in the economy of South Africa.

Furthermore another advantage of the Act is its dual objective, as this competition law is perceived to have exceed its scope of typical competition law as compared to laws of developed countries, as it aims to find a balance between the promotion of competition and development [39]. In addition, another advantage of this Act is that it takes into consideration aspects that are unique to South Africa's development, including but not limited to public interest issues such as empowerment, employment and SMEs [35].

Furthermore the establishment of three institutions (such as the competition commission, competition tribunal and competition appeal court) ensures that there are processes in place with regard to addressing anti-competitive conduct and as well as ensuring a fair trial amongst the parties which might be involved in competitive disputes.

Legh, Staples and Masamba [37] argued that while progress has been made by the competition commission in promoting and furthering the policy and its objectives, there are however some challenges. One of the challenges as noted by Legh, Staples and Masamba [37] is the competition commission authorities' failure to follow due process in enforcing the competition Act.

Furthermore it is of a view of a researcher that the South African Competition Act in its current form is more likely to cause issues with the emergence of cloud computing. This is corroborated by Luciano and Walden [41] as they have noted that competition law challenges are likely to emerge as cloud computing gains its maturity, however they are some areas currently which competition issues have started to emerge. These includes open standards and public procurement, interoperability and public procurement, as well as data portability and data protection.

5. CONCLUSIONS

From the discussion above, it is evident that cloud computing raises policy challenges that needs to be addressed by policy makers. A lack of policy that addresses cloud computing challenges can negatively have an impact on areas such as security and privacy, competition, intellectual property and liability, consumer protection, cross border and juridical challenges. Moreover, other categories identified by Yoo [42] which can have policy implications on the cloud includes Industry structure, Data Centers, Server-related technologies, Access networks and Regulations.

Some of existing policies and regulation reviewed, were enacted decades ago, thus raising a gap which needs to be covered in order to accommodate new technological developments. What is interesting is that such challenges are not only experienced by South Africa, as there are other countries who are stuck with legislation and policy documents that have been enacted decades ago. For instance, some privacy policy acts such as the United States Stored Communication Acts, was enacted decades ago and therefore not sufficient to handle regulatory issues that are being raised by the emergence of cloud computing.

The gap between policy and new technological developments is becoming so significant to a level that some argue that policies regarding information security should be rethought. Thus Cloud computing is very broad term and it is most likely to raise some policy questions which will need

to be addressed. From the discussion above and from a South African perspective, current policies and regulatory frameworks are not conducive enough to address all cloud challenges which impacts adoption of cloud computing services.

It is evident from the discussion above that there is a need for a cloud computing policy framework that adheres to international standards and that will address some of the pressing challenges emanating from the adoption and use of cloud computing. Moreover, there is a need for a well thought cloud computing policy that does not overregulate but addresses cloud challenges with the aim of improving public user confidence in the cloud and rapid adoption rate computing. Conversely, this policy should be interdisciplinary and should include factors such as competitiveness, finance, technology and law [43].

REFERENCES

[1] J. Kaur, A. Sehrawat, and N. Bishnoi. 2014. Survey Paper on Basics of Cloud Computing and Data Security. International Journal of Computer Science Trends and Technology, 2 (3), May 16-19.

[2] European Community for Software Services. 2010. "White Paper of Software and Service Architectures, Infrastructure and Engineering – Action Paper on the Area for the Future EU Competitiveness, "Volume 2: Background information, Version 1.3, [Online]. Available from http://www.euecss.eu/contents/documentation/volume%20two_ECSS%20White%20Paper.pdf [Accessed: 24/03/2011]

[3] National Institute of Standards and Technology (NIST). 2011. "The NIST Definition of cloud computing," Available from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Accessed: 20/03/2012].

[4] M. Carroll, A. Van der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls," Proceedings of the 2011 Information Security for South Africa (ISSA 2011) Conference, August 15-17, 2011.

[5] K. Junck and M. Rahman, "Cloud Computing avoids downfall of application service providers" in International Journal of Information Technology Convergence and Services, vol. 1, pp. 1-20, 2011.

[6] S. Ramgovind, M. Ellof, and E.Smith, "The management of security in Cloud computing," Information Security for South Asia (ISSA) [Online]. Available from: http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/27_Paper.pdf [Accessed: 15/04/2012].

[7] S. Garg and R. Buyya, Green Cloud computing and Environmental Sustainability. The University of Melbourne, 2011.

[8] G. Conway and E. Curry, "Managing Cloud Computing: A Life Cycle Approach," 2nd International Conference on Cloud Computing and Services Science, Porto, 2012.

[9] S. Chowhan and R.Saxena. Customer Relationship Management from the Business Strategy Perspective with the Application of Cloud Computing. In the Proceedings of DYNAA, 2011. vol. 2, no.1.

[10] L. Wenhao, "A community cloud oriented workflow system framework and its scheduling strategy," 2010 IEEE 2nd Symposium on Web Society (SWS), pp.316-325, 2010.

[11] S. Qureshi and M. Kamal. 2011. Role of Cloud Computing Interventions for Micro-Enterprise Growth: Implications for Global Development. In Proceedings of the Fourth Annual SIG GlobDev Workshop: Fourth Annual SIG GlobDev Workshop. Shanghai: Routledge, ISBN 978-0-9826068-2-7.

[12] S. Shahane, R. Kulkarni. 2014. Cloud Auditing: An Approach for Betterment of Data Integrity. International Journal of Soft Computing and Engineering, 3(6), Jan: 107-112.

[13] S. Bhardwaj, L. Jain, and S. Jain, "Cloud computing: A study of infrastructure as a service (IAAS)", International Journal of engineering and information Technology, vol. 2, pp. 60-63, 2010.

[14] M. Mujinga, B. Chipangura. Cloud computing concerns in developing economies. In Paper presented at the 9th Australian Information Security Management Conference, December 5-7, 2011.

[15] M. Ahmed, M. Hossain. 2014. Cloud Computing and Security Issues in the Cloud. International Journal of Network Security and Its Applications, 4(1), Jan: 25-36.

[16] International Telecommunication Union. Demystifying Regulation in the Cloud: Opportunities and Challenges for Cloud Computing. GSR12 Discussion Paper. October 2012.

[17] J. Sluijs, P. Larouche and W. Sauter. Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market, 3 (2012) JIPITEC 12, para 12.

[18] C.Hinde, JP Van Belle. 2012. Cloud Computing in South African SMMEs: Risks and Rewards for Playing at Altitude. International Research Journal of Computer Science Engineering and Applications, 1(1) October.

[19] BSA Software alliance. "2016 Global Cloud Computing Scorecard" [Online]. Available from: http://cloudscorecard.bsa.org/2016/pdf/BSA_2016_Global_Cloud_Scorecard.pdf [Accessed 20/06/2016] M. Patton. Qualitative evaluation and research methods. 3rd ed (Thousand Oaks, CA: Sage Publications, Inc., 2001).

[20] The Department of Justice. "Protection of Personal Information Act" [Online]. Available from: http://www.justice.gov.za/legislation/acts/2013-004.pdf [Accessed 10/06/2016].

[21] PwC. 2011. The protection of personal information bill: The journey to implementation.

[22] D. Kafouris. "Getting with the POPI programme" [Online]. Available from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=69449 [Accessed: 15/02/2016].

[23] M. De Villers, 2004. Consumer Protection under the Electronic Communications and Transactions Act 25 of 2002. Dissertation. Johannesburg: University of Johannesburg.

[24] Geredal, S.L. 2006, 'The Electronic Communications and Transactions Act' in Thornton, L (ed.) Telecommunications Law in South Africa

[25] J. Warner. 2011. Understanding Cyber-Crime in Ghana: A View from Below. 5(1), Jan-July: 736-749.

[26] F.W. Onifade and K.J. Adebayo. 2011. VDetector: Attacking the Attacker towards Combating Phishing and Identity Theft on the Internet. Journal of Information Technology Impact. 11(2): 133-144.

[27] I.Z. Dhlamini Cyber Security Awareness Initiatives in South Africa: A Synergy Approach [Online]. Available from http://researchspace.csir.co.za/dspace/bitstream/10204/5941/1/Dlamini_2012.pdf [Accessed 14/04/2015].

[28] A. Harris, S. Goodman and P. Traynor. 2013. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. Washington Journal of Law, Technology and & Arts. 8(3): 246-264.

[29] C. Erasmus, 2011. Consumer Protection in International Electronic Contracts. Mini-Dissertation. Potchefstroom: North-West University.

[30] S. Dara. 2013. Cryptography Challenges for Computational Privacy in Public Clouds. ACM, p.23- 33.

[31] N.S. Chauhan, A. Saxena, and J.V.R. Murthy. October 2013. An Approach to Measure Security of Cloud Hosted Application. In Proc. of IEEE CCEM 2013. Bangalore, India

[32] M. Chandramouli, R. Iorga and S. Chokhani,"Cryptographic key management issues and challenges in cloud services," NIST Report 7956, pp.1-31, 2013

[33] Marten van Dijk and Ari Juels. On the impossibility of cryptography alone for privacy preserving cloud computing. In Proceedings of the 5th USENIX conference on Hot topics in security, HotSec'10, pages 1–8, Berkeley, CA, USA, 2010. USENIX Association

[34] Z. Jobodwana. 2009. E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges. Journal of International Commercial Law and Technology. 4(4): 287-298

[35] T. Hartzenberg, Competition Policy and Practice in South Africa: Promoting Competition for Development Symposium on Competition Law and Policy in Developing Countries , 26 Nw. J. Int'l L. & Bus. 667 (2005-2006)

[36] South African Competition Commission. "Competition act no. 89 of 1998 [Online]. Available from http://www.compcom.co.za/wp-content/uploads/2014/09/pocket-act-august-20141.pdf [Accessed: 14/07/2015]

[37] R. Legh, J. Staples and M. Masamba. Competition Law Sibergramme [Online]. Available from: http://www.bowman.co.za/FileBrowser/ArticleDocuments/CompetitionLaw_SG_3_of_2012-2.pdf [Accessed: 23/04/2016]

[38] Organisation for Economic Co-operation and Development (OECD). Public Interest Considerations in Merger Control [Online]. Available from: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WP3/WD(2016)13&docLanguage=En [Accessed: 05/08/2016]

[39] F. Kronthaler and J.Stephan. 2006. Progressivity and Flexibility in Developing an Effective Competition Regime: Using Experiences of Poland, Ukraine, and South Africa for developing countries. Discussion Paper. Available from: http://nbn-resolving.de/urn:nbn:de:gbv:3:2-4380 [Accessed 08/07/2016]

[40] A. Török. Competition policy reform in South Africa - Towards the mainstream CP model for 'transition' economies in the Third World? [Online]. Available from: http://www.iwh-halle.de/projects/competition_policy/sa_country_study.pdf [Accessed 06/07/2016].

[41] I.Walden and L. Luciano. Ensuring Competition in the Clouds: The Role of Competition Law? (April 7, 2011) [Online]. Available from: SSRN: http://ssrn.com/abstract=1840547 [Accessed: 25/12/2015]

[42] C.S. Yoo. 2011. Cloud Computing: Architectural and policy implications, Review of Industrial Organization 38(4): 405–421.

[43] A. D. Helvacioglu-Kuyucu. 2011. Exploring Policy-Formulation for SMEs in Cloud Computing: The Case of Turkey. IBIMA Business Review. https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Cloud_Walden_5.pdf [Accessed 12/01/2016]

AUTHORS

Mpho J. Mohlameane was born in Pretoria on the 19th of September 1982. Mohlameane currently holds National Diploma in Software Development (2004), Bachelor Degree in Software Development (2010) and Master's Degree in Business Information systems (2012). All the qualifications were obtained from Tshwane University of Technology, Pretoria, South Africa. Mohlameane's major field of study is in information systems. He is current employed at State Information Technology Agency (SITA) as a Senior Software Developer.

Nkqubela L. Ruxwana was born in Eastern Cape on the 25th of December 1983. Dr. Ruxwana currently holds National Diploma in Engineering Computer Systems, Bachelor Degree in Computer Systems, and Masters in Information Systems from Tshwane University of Technology, Pretoria, South Africa. Dr. Ruxwana also holds Master's Degree in Business Leadership (University of South Africa) and a PhD in Information Technology from Nelson Mandela Metropolitan University (NMMU), South Africa. Currently he is a Professor and a Research Supervisor at Tshwane University of Technology, with extensive industry and research experience in the domains such as business analysis, strategy, project management, business intelligence, enterprise architecture, cloud computing, ICT4D, and health informatics.