PRIVACY AND SECURITY IN THE CLOUD: TANZANIA AND SOUTH AFRICA IN COMPARATIVE PERSPECTIVE

DOREEN FARIJI MWAMLANGALA

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY OF THE OPEN UNIVERSITY OF TANZANIA

2020

CERTIFICATION

The undersigned certifies that he has read and hereby recommends and approves for acceptance by the Open University of Tanzania a thesis titled; "**Privacy and Security in the Cloud: Tanzania and South Africa in Comparative Perspective**" in fulfilment for the degree of Doctor of Philosophy(PhD) of the Open University of Tanzania.

…….

Prof. Dr. Alex B. Makulilo

(Supervisor)

……

Date

DECLARATION

I, Doreen Fariji Mwamalangala, do hereby declare that this thesis is my own original work and that it has not been presented for similar or any other degree award at the Open University of Tanzania or any other university.

.....

Signature

.....

Date

COPYRIGHT

DEDICATION

To my beloved husband Fariji, our children Gwakisa and Sekela and my dearest parents, Andrew and Sarah Mshana, your endless prayers and support got me to where I am today. I cannot possibly thank you enough.

ACKNOWLEDGEMENTS

I thank and praise the name of the almighty God for His blessings and protection during the writing of this thesis to its completion. The completion of this research work is a result of encouragement, support, and assistance from different individuals in different ways and capacities. I would like to convey my honest appreciation to them all. Specifically, I would like to express my special appreciation to my supervisor, Prof. Dr. Alex B. Makulilo, who mentored me in every stage of the doctoral journey. I gained much from his readiness to share immense knowledge he has in research as well as academic writing in this area of law. Not only did he give merited criticisms and discerning comments, but also, used to draw my attention to necessary perspectives and issues, which I would have otherwise disregarded. I honestly admit that without his support and guidance, this work would not have reached this far.

I am so grateful to my husband, Fariji Mishael, our children, Gwakisa and Sekela for their love, trust, support, understanding as well as many sacrifices they made to make the completion of this work possible. Additionally, endless appreciation goes to my parents, Andrew Mshana and Sarah Mshana for their support, prayers, encouragement and all the sacrifices they made for my academic foundation and live hood from my childhood. I also cast thanks to my siblings and their families for moral and economic support all the way.

I wish to thank my employer, the Open University of Tanzania for exempting me some duties to allow me more time to focus on my PhD project. I also thank my colleagues

from the Faculty of Law, the Open University of Tanzania, who commented on my work and supported me morally towards the completion of this thesis.

ABSTRACT

The advantages of using cloud computing in day-to-day business attract and make many nations adopt it. However, the adoption of cloud computing is coupled with privacy and security concerns. These concerns raise questions as to what steps to be taken to enjoy the benefits of using cloud computing and at the same time uphold privacy and security in the cloud. This study seeks to address these concerns. It investigates legal challenges emanating from the use of cloud computing. It also interrogates the adequacy of the existing legal and regulatory framework in protecting privacy and security in cloud environment. Similarly, the relevancy of the international general principles and guidelines of the best practices in protecting privacy are assessed. The study employs mainly doctrinal legal research methodology which is supplemented by historical and comparative methods. The study is delimited to Tanzania and South Africa to gain a comprehensive insight of the subject matter of the study. After the consideration of the above issues this study has found that the existing legal and regulatory frame work does not accommodate the protection of privacy and security in cloud environment. Accordingly, the study recommends a law reform both in Tanzania and South Africa. Also this study recommends for adoption of other protection measures such as privacy by design and default.

TABLE OF CONTENTS

LIST OF CONSTITUTIONS AND LEGISLATION

Selected Treaties and other International and Regional Documents

APEC Privacy Framework, 2005.

AU Convention on Cyber security and Personal Data Protection, 2014.

Automatic Processing of Personal Data, 1981.

Directive 95/46/EC, of the European Parliament and of the Council, 1995.

EAC Legal Framework for Cyber Law 2008.

EU General Data Protection Regulation, 2016.

European Convention on Human Rights, 1950.

International Covenant on Civil and Political Rights, 1966.

Organisation for the Economic Co-operation and Development Guidelines on the Protection of Privacy and Trans-Border Data Flows of Personal Data, 1980.

SADC Model Law on Data Protection, 2012.

The Charter of Fundamental Rights of the European Union, 2010.

The Council of Europe Convention for the Protection of Individuals with Regard to The Supplementary Act A/SA.1/01/10 on Personal Data Protection, ECOWAS, 2010.

The Treaty Establishing the Constitution of Europe, 2004.

United Nation Guidelines for the regulation of Computerised Personal Data File, 1990.

Universal Declaration of Human Rights, 1948.

Constitutions

The Constitution of the United Republic of Tanzania of 1977 as amended from time to time.

The Constitution of South Africa, 1996.

South African Legislation

Children's Act, No. 38 of 2005.

Choice of Termination of Pregnancy Act, No. 92 of 1996.

Consumer Protection Act, No. 68 of 2008.

Electronic Communication Act, No. 36 of 2005.

Electronic Communications and Transactions Act, No. 25 of 2002.

National Credit Act, No. 34 of 2005.

National Health Act, No. 61 of 2003.

Promotion of Access of Information Act, No. 2 of 2000.

Protection of Personal Information Act, No. 4 of 2013.

Regulation of Interception of Communication and Provision of Communication-related Information Act, No. 70of 2002.

Tanzanian Legislation

Cyber Crimes Act, No 14 of 2015.

Electronic and Postal Communication Act, No 3 of 2010.

Electronic and Postal Communication (Consumer Protection) Regulations, 2018.

Electronic and Postal Communication (Online Content) Regulations, 2018.

HIV and AIDS (Prevention and Control) Act, No 28 of 2008.

Human DNA Regulation Act, No 8 of 2009.

The Medical, Dental and Allied Health Professionals Act, No 11 of 2017.

Prevention of Terrorism Act, No 19 of 2002.

Registration and Identification of Persons Act, (Act No 11 of 1986) R. E2002.

Tanzania Intelligence and Security Act, (Act No 15 of 1996) R.E. 2002.

LIST OF CASES

Tanzanian Cases

South African Cases

LIST OF ABBREVIATIONS AND ACRONYMS

ALL SA	All South African Law Reports
AIDS	Acquired Immunodeficiency Syndrome
APEC	Asia-Pacific Economic Cooperation
AU	African Union
AWS	Amazon Web Services
BCLR	Butterworth's Constitutional Law Reports
CBPR	Cross Border Privacy Rules
CEIR	Central Equipment Identification Register
CFR	Charter of Fundamental Rights of the European Union
COE	Council of Europe
CPA	Consumer Protection Act
CSP	Cloud Service Provider
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
DPO	Data Protection Officer
EAC	East African Community
EASSy	Eastern African Submarine Cable System
EC	European community
ECA	Electronic Communication Act
ECOWAS	Economic Community for West African States
ECHR	European Convention on Human Rights
ECTA	Electronic Communication Transaction Act
EC2	Elastic Compute Clouded(s)editor

EPOCA	Electronic and Postal Communications Act
Et al.	*et alia* (and others)
EU	European Union
G- Cloud	Government Cloud
HC	High Court
HIPSSA	Harmonization of the ICT Policies in Sub- Saharan Africa
HIV	Human Immunodeficiency Virus
HRC	Human Right Committee
IaaS	Infrastructure –as-a-Service
IBM	International Business Machine
Ibid	*ibidem*(in the same place)
ICASA	Independent Communication Authority of South Africa
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICT	Information and Communication Technology
IDG	International Data Group
IPPs	Information Privacy Principles
IT	Information Technologies
ITU	International Telecommunication Union
LGAs	Local Government Authorities
LRCT	Law Reform Commission of Tanzania
MDAs	Ministries Department and Agencies
NCA	National Credit Act
NICTBB	National ICT Broadband Backbone

NIST	United States National institute of Standards and Technology
No	Number
OECD	Organisation for Economic Co-operation and Development
OWASP	Open Web Application Security Project
PaaS	Platform-as-a-Service
PAIA	Promotion of Access to Information Act
POPI	Protection of Personal Information Act
RICA	Regulation of Interception of Communication and Provision of Communication Related Information Act
S	Section
SA	South African Law Reports
SaaS	Software-as-a- Service
SAP	Systems Applications and Products
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SCA	Supreme Court of Appeal of South Africa
SEACOM	Southern and Eastern African Communication Network
SLA	Service Level Agreement
SMEs	Small and Medium- size Enterprises
Supra	Previously cited
TCRA	Tanzania Communication Regulatory Authority
TISS	Tanzania Intelligence and Security Services
T.L.R	Tanzania Law Report
UDHR	Universal Declaration of Human Rights

UN	United Nations
US /USA	United States of America
USD	United States Dollar

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Study

Security and privacy have been a human concern since the earliest Greek civilisations. However, the rise and development of Information and Communication Technologies fuelled the concern in today's society. The presence of cloud computing increases the concern because the size and amount of data that can be collected is very huge, at a high speed and with a vast storage capability. Similarly, the manipulation possibilities have increased, and personal data can be shared easily in the cloud as well as in social media. Thus, technologies are coupled not only with enormous benefits but also with many security and privacy concerns.[1]

Correspondingly, the dialogue of privacy protection has developed slowly over years. Record keeping upon individuals (the reason that led to the emergence of data privacy regulation) is regarded to be as old as human civilisation.[2] Nevertheless, the current concept of data protection and privacy traces its origin from the article known as "the Right to Privacy", that was published in 1890 in Harvard Law Review.[3] Moreover, it was between 1960s and 70s that tangible privacy and data protection regulation came into being.[4] Since late 1960s a number of international agencies such as the Council

[1]Ardent, H., The Human Condition, 2nd Ed, Chicago, the university of Chicago Press. 1958. pp 5.

[2] Bennett, C. J., Regulating Privacy: Data Protection and Public Policy in Europe and United States, Cornell University Press, Ithaca/London, (1992). pp. 18.

[3] Warren, S. D., & Brandeis, L. S. *The Right to Privacy, Harvard Law Review*, 1890, Vol 4, No 5, pp. 193-195; The work has traditionally and frequently been cited in many scholastic writings that deals with the history of the Right to Privacy. It is regarded by many as the official birth date of the right to privacy in the world.

[4]Makulilo, A. B. Protection of Personal Data in Sub-Saharan Africa, PhD Thesis, University of Bremen, 2012.

of Europe and the Organisation for Economic Co-operation and Development (OECD) were active in the field of privacy and data protection.[5]

In fact, the first data protection regulation at the national level was made in the German state of Hesse in 1970.[6] Similarly, in 1973 Sweden made its first Data Protection Act.[7] This was unsurprisingly so because the period marked the development in computer and communication technology. Development of modern technologies particularly the internet and cloud computing made it feasible for organisations be they private or public and even individuals to process personal data that might interfere with personal privacy.[8] Moreover, the legal response to the protection of personal data and privacy in ICT world had been to enact data protection legislation.[9]

Additionally, Pearson and Yee posit that at the widest level, privacy is a fundamental human right enshrined in the United Nations Universal Declaration of Human Rights (1948) and later in the European Convention on Human Rights and National Constitution and Charters.[10] Formally, the primary focus of privacy regulation was to protect personal information of individuals against government surveillance and impending compulsory disclosure of private information in databases. With the development in computer and information technology the concerns shifted to protection of privacy against direct marketing and telemarketing. With the rise of

[5]Lloyd, I. J., Information Technology Law, 8th Edition, Oxford University Press, Great Clarendon Street, United Kingdom. 2017 pp. 32
[6]Ibid. p. 31
[7]Ibid.
[8]Makulilo. Note 4, supra.
[9]Roos, A., The Law of Data (Privacy) Protection: A Comparative and Theoretical Study, LLD Thesis, UNISA, 2003, pg. 17
[10]Pearson, S. & Yee, G., Privacy and Security for Cloud Computing, Springer International Publishing, Springer- Verlag –London, 2013.

cloud computing the consideration is given to the increasing risk of online identity theft and spamming.[11]

The term cloud computing is a paradigm shift in the way in which information is managed and consumed.[12] It has become a new way of distributing and acquiring IT services in which computing services such as software, storage, databases, servers and networking.[13] Apparently, the impact of cloud computing is escalating and it is receiving an increasing attention in scientific, academia and business societies.[14] Its adoption leads to more innovation, improving cost efficiency and scalability of applications to meet the demand.[15]

The end user does not need a software or server to access information. He/she only needs internet connection because the server and the software management are accessed from the cloud under the management of the cloud service provider.[16]Many people are customers of cloud computing through services such as online searching, 'whatsapping', online streaming and many others.[17]Examples of cloud service

[11]Ibid, p. 12.
[12]ITU, Privacy in the Cloud. ITU-Technology Watch Report, Geneva, 2012. Accessed from https://www.itu.int/en/ITU-T/techwatch/PAges/cloud-computing-privacy.aspx, on 12th December,2016.
[13]Bhawan, L, N., *Legal and Policy Issues in Cloud Computing*, a discussion Paper based on DSCI-BSA Workshop, 2013. Data Security Council of India. Accessed from http://www.dsci, on 12th December 2016.
[14]Hashzume et.al., *An Analysis of Security Issues for Cloud Computing*. Journal of Internet Services and Applications, 4.5., 2013. Accessed from http://www.jisjournal.com/content/4/1/5, on 12th December 2016.
[15]Sen, J., *Security and Privacy Issues in Cloud Computing*, in Ruiz-Martinez et.al. (eds) Architectures and Protocols for Secure Information Technology, IGI- Global Publishers, USA, pp 1-45, 2013.
[16]Goel, A. &Goel, S., Security Issues in Cloud Computing. International Journal of Application or Innovation in Engineering & Management, 2012, Vol 1, Issue 4. Accessed from http://www.ijaiem.org/volume1/issue4/IJAIEM-2012-12-26-033.pdf, on 12th December 2016.
[17]Kong et.al. *Introduction to Cloud Computing and Security Issues*, in Cheung A., S., & Weber, R., H., (ed) Privacy and Legal Issues in Cloud Computing, Edward Elgar Publishing Limited, Cheltenham, United Kingdom, 2015.

providers include Google, Yahoo, Ubuntu, Microsoft, IBM and Amazon to mention just a few.[18]

Furthermore, the spending in cloud computing globally has been growing at the rate of almost six times more than the rate spent on IT.[19]The spending was mostly on software-as-a-service (SaaS). However, the trend is changing due to change in market requirements. The market now adopts the use of platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) more.[20] Similarly, according to the survey done by the International Data Group (IDG) in some selected African countries,[21] it was discovered that the use of cloud computing is highly embraced.[22] The evidence is that some workloads and services have been moved either to the cloud platform, software as a service or to cloud hosted infrastructures; and many more are underway.[23]

Comparatively, African market is relatively immature compared to European market for cloud computing services.[24] A study done by System Applications and Products (SAP) and IDG showed that there is more development in technology and establishment of technological centres as well as the presence of impending

[18]Barbara, J., J., Cloud Computing: Another Digital Forensic Challenge, 2009. Accessed from http://www.dfnews.com/articles/2009/10/cloudcomputing-another-digital-forensic-challenge, on 27th December 2016.

[19] Lavelle, M., Why the shift to cloud computing Reminds me of the Ford Model-T? 2016 Accessed from http://www.linkedin.com, on 26th December 2016.

[20] Ibid, pg. 2.

[21] The survey was done to some African countries such as Algeria, Kenya, Morocco, Nigeria and South Africa. It was discovered that most of the organizations in those countries have already embraced the use of cloud computing.

[22] Hill, K. Cloud Computing Emerging in Africa, 2015 Accessed from http://www.rcrwireless.com/ 20151023/featured/cloud-computing--in-africa-tag6, 0n 26th December 2016.

[23] Ibid, p. 7.

[24] Ibid, p. 8.

advantages of adopting cloud computing, than it were before.[25]Consequently, African continent is ready for adoption of cloud computing.[26]

Similarly, Mukami posits that it is an evolving truth that Africa aspires of more data driven economies and the technology which cloud transformation can realize.[27] The observation implies that in technological perspective, Africa is ready to adopt cloud computing. However, a question remains, is Africa ready in legal perspective for the espousal of cloud computing? The question arises due to the fact that only 22 countries out of 53 have enacted the omnibus data protection laws that provides for the security and privacy in the cloud.[28] This study was therefore intended to find answers to this question. In doing so; it only focused on the legal framework and challenges of privacy and security in the cloud, by comparing Tanzanian and South African perspectives.

Notably, Tanzania as many other countries follow the world trend in adopting cloud computing. That is clearly shown by the deployment of the National ICT Broadband Backbone (NICTBB) as well as the landing of two submarine cables.[29] These are Southern and Eastern Africa Communication Network (SEACOM) and the Eastern Africa Submarine Cable System (EASSy).[30]The above initiatives facilitated the

[25]Ibid.
[26] Ibid, p. 9.
[27]Mukami, S., Technology: We Need to Embrace Cloud Computing, 2017. Accessed from http://www.potentash.com/2017/03/21/embrace-cloud-computing/, on 8th August 2017.
[28]Greenleaf, G., *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*. 145 Privacy Laws & Business International Report 10 [2017] UNSWLRS 45. Accessed from http://www.austlii.edu.au/au/journals/UNSWLRS/ on 24th April 2019.
[29]Esselaar, S. & Adam, L. (2013) Understanding what is happening in Tanzania: Evidence of ICT Policy Action, Policy Paper II. Accessed from http://www.researchICTafrica.net, on 28th April 2017
[30]Ibid.

availability of high capacity broadband connections to other parts of the world and hence promoting the use of cloud computing.

Furthermore, the government promote the use of ICTs, cloud computing inclusive in the work place. This was accelerated by the establishment of ICT units in Ministries Department and Agencies (MDAs) as well as in Local Government Authorities (LGAs). The same is adopted in Micro and Small Medium Enterprises (SMEs) and the private sector.[31] This implies that the country has an experience of cloud computing at different levels. At regulatory level, the right to privacy is protected through article 16 of the Constitution,[32] and in some sectoral laws.[33]Yet, there is no specific or an omnibus law that provides for data protection.[34]There are also a number of laws and regulations that were made under the National ICT Policy (NICTP), 2003 for promoting electronic commerce,, protecting consumers and addressing cybercrime challenges. However, they did not address privacy issues.[35]Consequently, the NICTP 2003 was revised and renamed NICTP 2016 to include privacy and security element.[36]

Correspondingly, South Africa is regarded as one of the leading countries in Africa in

[31]The United Republic of Tanzania, Ministry of works, Transport and Communication, National Information and Communications Technology Policy, 2016, Accessed from http://www.Tanzict.files.wordpress.com, on 28th April 2017.
[32]The Constitution of the United Republic of Tanzania, 1977.
[33]These include Cyber Crimes Act, 2015, Electronic and Postal communications Act, 2010, HIV and AIDS (Prevention and Control) Act, 2009, Medical Practitioner Act, 2002, Prevention of Terrorism Act, 2002, Registration and Identification of Persons Act, 2002, Tanzania Intelligence and security Act, 1996.
[34]ITU, Cloud Computing in Africa- Situation and Perspectives, 2012. Accessed form https://www.itu.int/en/publications/ITU-D/Pages/pudlications.aspx?parent=D-PREF-THEM.07-2012&media=electronic, on 28th April 2016.
[35]These laws are Electronic and Postal Communication Act, No 3 of 2010, Universal Communication Act of 2006 and Cybercrimes Act, 2015 accessed from http://www.itu.int>ITU-D>treg>publications, on 28th April 2017.
[36]The United Republic of Tanzania, Ministry of Works, note 31, supra. pg. 5.

using cloud computing.[37] At regulatory level, privacy right is protected firstly, under common law, and secondly by article 14 of the country's Constitution.[38] There is also a specific legislation for privacy protection, known as the Protection of Personal Information Act, 2013, (POPI). This law upholds privacy right as provided in the Constitution.[39] It also provides guidelines on how to protect that right. POPI is aligned to the 1995 European Data Protection Directive (Directive 95/46/EC) as well as the contemporary international best practices and laws on privacy protection.[40]However, despite POPI legislation in place, only a few of its sections have come into effect. These include sections that provide for the establishment of the office of the information regulator as well as the definitions section.[41] This implies that privacy right though accepted and upheld by this law, is not legally and properly protected, going by the observation that most of its sections for protection are not yet effected.

1.2 Statement of the Problem

Different experts have raised concerns about security and privacy in cloud computing adoption and use.[42] The Cloud Security alliance in 2013, for instance, identified data breaches and data loss as areas of concern regarding cloud computing.[43] The former

[37]Gillward et al., The Cloud Over Africa, 2013.Accessed from http://www.researchictafrica.net/publications, on 2nd May 2017.
[38]Roos, A., *Data Protection Law in South Africa*, in Makulilo, A. B. (ed) African Data Privacy Laws, Switzerland, Springer International Publishing AG, 2016, pp. 189-228.
[39] Ibid.
[40]Michalson, L. Data Privacy or Data Protection in South Africa,2013. Accessed from http://www.michalson.com, on 28th April 2017.
[41]DLA Piper, Data Protection Laws of the World, South Africa, 2017. Accessed from http://www.dlapiperdataprotection.com, on 29th April 2017.
[42]Njue, D., Cloud Services Opportunities and Challenges for East Africa, 2013. Accessed from http://www.slideshare/itnewsafrica/cloudservices, on 26th December 2017.
[43]Samson, T., 9top Threats to cloud Computing Security, 2013. Accessed from http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428?page=0,0&source=footer, on 11th September 2017.

refers to the release of protected information that includes personally identifiable information, financial information, personal health information and the like to an untrusted environment either intentionally or unintentionally.[44] When this security incident happens, sensitive, personal and protected data are copied, stolen, viewed, communicated or used by someone not authorized to do so.[45] Likewise, data loss is another security issue which threatens cloud computing. It includes deletion of data by malicious hackers, natural or human induced calamities as well as by unconcerned cloud service providers (CSPs).[46]Likewise, security and privacy challenges in the cloud computing are caused by a lack of control by cloud service consumers.[47] That is, their data are stored in the cloud infrastructures that are managed, owned, and operated by the service providers within the territory or in other jurisdiction.[48] This poses threat to data security, privacy, integrity and confidentiality principles.

To address the problem of a lack of security and privacy in cloud computing there has been some efforts in place. The legislation in EU on data protection, for example, has served as the key point of departure for the development of national data privacy regimes in different parts of the world as well as the best practises.[49] International Telecommunication Union (ITU) also issued reports and proposals for the best

[44]Kong et al., *Introduction to Cloud computing and Security Issues*, in Cheung, A. S. Y. & Weber, R. H., (ed) Privacy and Legal Issues in Cloud Computing, Edward Elgar Publishing Limited, Cheltenham, United Kingdom, 2015. pp 17.
[45]Ibid.
[46]Ibid, pg. 17.
[47]Turahi, D., Security and Privacy: Can We Trust the Cloud? 2013. A paper presented in East African Information conference in Kampala Uganda on 13th to 14th August, 2013. Accessed from https://www.isaca.org/chapters2/kampala/documents/Security%20and%20Privacy%20in%%20the%20cloud.pdf, on 27th December 2017.
[48]Kauba, C. & Mayer, S. When the Cloud Disperse: Data Confidentiality and Privacy in Cloud Computing,2013. Accessed from http://www.uni-salzburg.at/teaching/sal/p, on 27th December 2016.
[49]Bygrave, L. A., Data Privacy Law-An International Perspective, 1st Edition, Oxford university Press. pp 265.

practice of security and privacy in cloud computing. Similarly, Madrid Resolution[50] provides for the standards accepted worldwide for data privacy and security protection.[51]

In June 2014, African Union member states adopted the African union Convention on Cyber Security and Personal Data, which also aims at protecting data security and privacy.[52] The problem is however that these guidelines, terms and agreements are not universally binding.[53] As a result, there is lack of legal harmony across regimes for enhancing data security and privacy in cloud environment.[54] That is, almost every state has its own municipal legal regime for cloud computing. The preliminary survey showed that legislation for data security and privacy in the cloud is different between Tanzania and South Africa despite being both southern African countries.

The preliminary information suggested that Tanzania depends mainly on technical protection of data rather than legal protection of privacy and security. In South Africa, privacy legislation known as the Protection of Personal Information Act, 2013 (POPI)[55] exists. Nonetheless, only sections dealing with definitions and the appointment of the information regulator have come into effect.[56] Similarly,

[50]This is a joint proposal for a Draft International Standards on the Protection of Privacy with regard to the processing of Personal Data, which was welcomed by the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5th November, 2009.

[51]ITU, Privacy in Cloud Computing, 2012. ITU-Technology Watch Report, Geneva. Accessed from http://www.itu.int/en/ITU-T/techwatch/pages/cloud-computing-privacy.aspx, on12th Dec 2016.

[52]African Convention on cyber Security and Personal Data was adopted by the 23rd ordinary session of the assembly of the African Union on 27th June 2014, in Malabo, Guinea. The Convention covers a wide range of online activities such as cyber security, cybercrime, data protection and electronic commerce.

[53]Ibid, p. 8.

[54]Ibid.

[55]Ross, note 38, supra.

[56]The south African President signed a proclamation in April 2014 declaring only some sections of the Act to be effective.

sluggishness in adopting available international security and privacy recommendations is also observed. For example, while African union member state adopted the African Union Convention on Cyber Security and Personal Data in June 2014,[57]however, only two country has ratified it to date, although 10 countries have signed it. This has deterred the application of the Convention considering that it requires the ratification of fifteen (15) member countries to enter into force.[58]

The foregoing elucidation explains the nature and the extent of the problem that this study sets out to investigate - security and privacy protection of privacy in the cloud. The consequence has therefore been threat to data security and privacy and hence the slow pace and unwillingness to adopt cloud services. The study draws examples from Tanzania and South Africa in comparative perspective with the intention of exposing the status of legal framework and mechanisms for privacy protection in cloud computing.

1.3 Research Objectives

The following objectives guided the present study:

1.3.1General Objectives

The main objective of this study was to investigate the legal challenges involved in the use of cloud computing with regard to security and privacy of information and suggest how it might be curbed to provide privacy and security in the cloud in

[57]African Convention on cyber Security and Personal Data was adopted by the 23rd ordinary session of the assembly of the African Union on 27th June 2014, in Malabo, Guinea. The Convention covers a wide range of online activities such as cyber security, cybercrime, data protection and electronic commerce.

[58]Access now Policy Team, African Union Adopts Framework on Cyber Security and data Protection, 2014. Accessed from https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection, on 23rd October 2017.

Tanzania and South Africa respectively.

1.3.2Specific Objectives

In order to achieve the general objectives of the study the following specific objectives guided this research:

i. to examine the legal challenges of privacy and security in cloud computing.
ii. to analyse the adequacy, relevancy, and appropriateness of the existing legal framework for privacy and security in Tanzania and South Africa and to establish the extent to which they recognise and tackle challenges arising from cloud computing.
iii. to analyse the accepted general principles and guidelines of the best practices on privacy protection, and suggest a framework for protecting privacy in the cloud in Tanzania and South Africa.

1.4 Research Questions

This research study intended to answer the following questions:

i. what are the legal challenges emanating from the use of cloud computing?
ii. how relevant, adequate and appropriate are the existing legal and regulatory framework and practices protect privacy and security in the cloud in Tanzania and South Africa?
iii. to what extent are the general principles and guidelines of the best practices relevant in protecting privacy and security in the cloud in Tanzania and South Africa?

1.5 Literature Review

There is a dearth of literature that discuses and makes comprehensive examination specifically on security and privacy in the cloud computing in Tanzania and South Africa. Although several authors have written on this subject most of the literatures are foreign to Africa. The review of the few literatures available undertaken in this study discloses that there are two schools of thought dealing with protection of privacy and security in the cloud.

The first school of thought advances the use technological means in their different studies and scholarly writings as a means of providing privacy and security of personal information in the cloud. They advocate for the use of different mechanism trying to limit access of personal information in the cloud, how and when. This is equivalent to what Lessig was referring to as privacy by code.[59]Additionally, there is a second group of thought in which scholars are advancing protection of privacy through legal mechanism. They advocate for using legal framework to control access to personal information and time and manner of accessing personal information. They also advance the use of sanctions in protecting privacy and security of personal information.

The scholars who argue in favour of technological measures in solving privacy and security issues in the cloud include Meetei and Goel, Takabi and Hashzume. Meetei and Goel posit that cloud computing has different architectures depending on services they provide.[60]According to them, cloud computing brings about new challenges on

[59]Lessig, L., Code, 2006. Basic Books, New York, 2006.

[60]Meetei, M. Z. & Goel, A., Security Issues in Cloud Computing, in 2012, 5th International Conference on Biomedical Engineering and Informatics (BMEI), pp 1321-1325. Accessed from http://www.researchgate.net/publication/261153895_Security_issues_in_cloud_computing, on 14th November 2017.

security and privacy that were not present in the traditional computing system. They mention some risks coupled with the use of cloud computing and legal risk being among them. These include data storage challenges,[61] data transmission challenges, application security, security of cloud integrity, and security challenges related to third party resources. They posit that in adopting cloud computing security mechanisms should be put in place for smooth running.

Although a number of authors are in agreement with Meetei and Goel, other scholars dissent. Takabi and his fellow scholars, for instance, in analysing the security and privacy challenges in cloud computing environment, dissent that though it is important to rely on technical means in providing privacy and security in the cloud, technical means alone are not enough.[62] They argue that legal mechanisms for data security and privacy protection must be embedded in all security solutions.

Correspondingly, there is a category of scholars who advocate for the legal mechanisms for privacy and security in the cloud. These include Ramgovind and his fellow scholars who argue on the quest for a legal framework for cloud computing together with technical mechanisms for privacy and security.[63]The authors posit that the modern-day technology of cloud computing compels cloud computing customers to rely on the third-party service providers on data security. This poses a problem as

[61]Customers store their data in the cloud and hence do not possess them locally anymore.

[62]Takabi, et al., Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy Journal, 2010, 8(6), 24-31. Accessed from http://www.asu.pire.elsevier.com/en/publications/security-and-privacy-challenges-in-cloud-computing-environments, on 29th December 2016.

[63]Ramgovind, et al., The Management of security in Cloud Computing 2010. A paper presented in Information Security for South African Conference in Johannesburg. Accessed from http://www.unisa.pure.elsevier.com, on 28th December 2017.

the only legal agreement in that relation is the Service Level Agreement (SLA), which according to them is not enough.

The same view is shared by Turahi, who argues that a regulatory institution is among the security and privacy challenges facing cloud computing.[64] According to him, the current practice of depending on the service provider for data privacy and security leads to legal quagmire and transitive trust on establishing who is accountable in complying with regulation if the services are subcontracted to a third-party cloud.[65]He proposes forming a legal framework for cloud computing which encompass data protection, trust, and privacy policies.

Although cloud computing is different from traditional computing, King and Raja express that regulations for cloud computing are necessary to reach the potentials of cloud computing.[66] The regulations, among other things, should focus on privacy and security of sensitive consumer data. They suggest that to achieve the above-named goal, laws are to be revised to offer heightened privacy and security of personal data in the cloud environment. They are of the view that there is the need to reform privacy laws to lay a firm regulatory foundation for the growth of cloud computing.

Furthermore, Adrian contends that the potentials brought about by cloud computing pose an enormous risk to privacy and security.[67]These potentials include among others, the way in which information may be collated, managed, stored, controlled,

[64]Turahi, note 47, supra.
[65] Ibid.
[66] King, N. J. and Raja, V. T., Protecting the Privacy and Security of Sensitive Customer Data in the Cloud, computer Law and Security Review, 2012, v. 28, pp 308-319. Accessed from http://www.sciencedirect.com, on 14th November, 2017.
[67]Adrian, A., How Much Privacy do Clouds Provide? An Australian Perspective, Computer Law and Security Review, 2013, v. 29, pp 48-57. Accessed from http://www.sciencedirect.com, on 5th December 2017.

and manipulated. The author posits that the right to privacy in the cloud, to some extent, is protected by the existing laws, some of which are not specific for the cloud. However, she advocates that privacy and security in the cloud are under countless threat owing the development in technology. The scholar is of the view that it is very unfortunate that the available legal framework is inadequate to secure privacy. She cites also Solove, who maintains,

> *The problem is caused in significant part by the law, which has allowed the construction and use of digital dossiers without adequately regulating the practices by which companies keep them secure.*[68]

In this sense, cloud computing calls for legal innovation according to Adrian above. Maaref, in the ITU report on situation and perspectives on cloud computing in Africa argues in accord with the above authors.[69] He for example, provides that in some African countries cloud computing is already in use as a solution for IT under equipment problem. Moreover, there are prospects for more development in adoption and implementation of the technology if some accompanying measures are taken into account timely. These measures include, but not limited to legal and regulatory mechanisms. The author also highlights that in regulatory level, more than half of African countries do not have legislation on data protection or any agreement with other countries on this regard, except some few countries.

Similarly, the scholar also posits that African leaders agree that there is a dire need to have regulatory environment that meets the international standards. Agreements

[68]Solove, D., *The New Vulnerability: Data Security and Personal Information*, in Chandler, A. et al, Securing Privacy in the Internet Age, Berkeley, CA, Stanford University Press, 2008.

[69]Maaref, S. ITU, Cloud Computing in Africa: Situation and Perspectives, 2012. Accessed from http://www.itu.int/ITU-d/treg/publications, on 2nd January 2017.

regarding personal data protection and data transfer security are necessary for the proper adoption and implementation of cloud computing. Likewise, the author suggests that there is the need to improve the legislative as well as regulatory framework. Such improvements can mitigate the challenges facing the migration to the cloud environment, and maintain conformity with international standards as well as the best practices in the field.

Besides, Gillward and his fellow authors in their article titled, Cloud over Africa, analysed cloud computing in five selected African countries which are Ghana, Nigeria, South Africa, Kenya, and Tunisia.[70] The scholars posit that cloud computing in these nations is still in infancy stages of growth except South Africa where there is higher rate of cloud activities. Similarly, the authors claim that security and privacy are among the factors hindering the growth of cloud computing in most of the developing countries in Africa. Likewise, they provide that although cloud computing falls within ICT framework, in ICT regulations there is no special provisions providing for cloud services in all selected countries. They recommend for the enactment of data security and privacy protection legislation in all the countries.

Equally, the above stand is shared by Omwansa and his fellow authors in a baseline survey of cloud computing in which they made an analysis of cloud computing in Kenya.[71] They are of the view that cloud technology can be adopted and properly implemented if there is proper legal and supportive framework. The authors posit that

[70]Gillward et al, note 37, supra.

[71]Omwansa, T. K, Waema, T. M. & Omwenga, B. Cloud computing in Kenya, A 2013 Baseline Survey, 2014. Accessed from http://www.c4dlab.ac.ke/uploads/2014/4, on 3rd January 2017.

the question of security and privacy of data in the cloud is one of the biggest challenges affecting cloud computing. In their report, they recommend that the ICT policy as well as the legal framework should be reviewed and make it flexible and effective to promote cloud computing. They also advocate for the need of specific laws to ensure the protection of consumers and end users of cloud services. They also argue that sometimes it is not necessary to have a specific law providing for cloud computing, but aspects relating to cloud computing should be clearly added and provided for in the existing law through amendment. These aspects include but not limited to data protection, information security, privacy, cybercrime, and conflict resolution for cloud environment.

In general, reviewing the above literature clearly portrays that privacy and security are a serious challenge brought about by cloud computing. Consequently, the need to have a legal protection for privacy and security is evident. It is also depicted that privacy and security protection in the cloud is not properly regulated for. However, the minds are still troubled on the fact that there is no consensus whether to have a specific law for cloud computing or to amend the existing law so as to accommodate and provide for the challenges brought by cloud computing. Moreover, the reviewed literature has not covered the parameter that this research intended to cover. The literature is silent on the topic of privacy and security issues in the cloud in Tanzania. Little seems to have been said in relation to the same topic for South Africa.

However, even the South African status is not discussed in detail. Moreover, the literature is silent on what to be done in the developing countries to protect privacy and security in the cloud for the interest of the internet community universally.

Therefore, there is apparent dearth of legal literature in Africa on data security and privacy in the cloud computing. These are the lacunas that the author has filled to provide a clear understanding of the existing situation in Tanzania and South Africa and be able to add in the pool of knowledge and provide supportive environment for privacy and security in the cloud.

1.6 Research Methodology

The study employed qualitative legal research approach and doctrinal legal research methodology. The study also supplemented the methodologies with historical legal approach and comparative methods. The doctrinal legal research method entails the analysis of primary and secondary sources of law. The methodology was used to analyse literature on privacy and security issues in the cloud and appraise the existing legislation on the subject matter. The rationale for using this methodology is expressed in latin maxim as "*lexlata*" and not "*lexferenda*". That it is regarded as the main legal methodology which focuses primarily on what a law is in a particular area and not what it ought to be.[72]

Correspondingly, the methodology extends from the textual examination of statutory provisions and case laws to exploration of legal scholarly works with the intention of proposing a legal reform which is part of the law as it ought to be or the "*lexferenda*" aspect. As a matter of fact, it is the method that is tremendously used in similar legal

[72]Dobinson, I. and Johns. F., '*Qualitative Legal Research'* in McConville, M., and Wing, H. C., (eds) Research Methods for Law, Edinburgh University Press, Edinburgh) 2007, pp18-19.

studies.[73] In addition to what is previously mentioned, the methodology was used to evaluate relevant literature on the subject matter of the study.[74]

Additionally, it facilitated the critical legal examination of relevant legislation, policies, case laws, international and multilateral instruments', reports, treaties, government reports, protocols, thesis, journals, books and international information security and privacy standards that are the primary and secondary sources of data. The researchers' main goal was to locate, collect the law that includes legislation and case laws, and apply them to a specific set of material facts with the intention of solving a particular legal problem.

Specifically, under this methodology, the researcher's intention was to analyse the existing legislation, model laws, reports, case laws, and other publications and assess how they relate to the subject of the study. It necessitated the use of different legal methods including inductive and deductive legal reasoning as well as rules of statutory interpretation to critically analyse the collected materials against the backdrop of the research questions. Specifically, this methodology was selected to answer one of the research questions, which require an examination of data security, and privacy legal challenges arising from the use of cloud computing.

[73]Masoud, B. S., Legal Challenges of Cross-Border Insolvencies in Sub- Saharan Africa with References to Tanzania and Kenya: A Framework for Legislation and Policies, PhD Thesis, University of Nottingham Trent, 2012.
[74] Singhal, A. K. & Malick, I.*Doctrinal and Social Legal Research Methods: Merits and Demerits*, Educational Research Journal, 2012, Vol 2 (7), pp 252-256.

Moreover, this methodology was very appropriate in this study owing to its potentiality in giving rise to the growth, continuity, tenacity, and certainty of law. The application of this methodology made it possible for this study to make an analysis of the existing legislation relating to security and privacy of data. It also enabled the study to ponder on how the law ought to tackle the emergence encounters and risks. It also facilitated the analysis, discussion and recommendation which promotes innovation and development of more privacy regulation. Moreover, through application of legal interpretation and analysis, this methodology aided in formulating recommendations that can be applied in Tanzania and South Africa.

Accordingly, the researcher made use of historical, analytical, and perspective approach to analyse different pieces of law.[75]Historical legal research involve among other things, the study of the historical growth of a certain legal principles or legal establishments or legal profession.[76]Through historical legal research, the researcher traced the historical predecessor of security and data privacy agreements and legislation. The focus was on what were the main issues that made the data security and privacy law to emerge? What were the conditions and mischief that were supposed to be cured by that particular law? The rationale behind this approach was to ascertain whether the mischief and issues that led to the emergency of that law were still relevant to data security and privacy in cloud computing environment. Besides, the researcher analysed on whether the existing legal framework carters for security and privacy

[75]Kiunsi, H., B., Transfer Pricing in East Africa: Tanzania and Kenya in comparative Perspective, PhD Thesis, the Open University of Tanzania, 2017.
[76]Taylor, L., Writing a Legal Research Paper- Research methodologies, in Scragg, J., et.al. (eds), Legal Writing: A Complete Guide for a Career in Law, LexisNexis, New Zealand, 2014.

issues in cloud environment. Also, the researcher critically examined how and to what extent the existing legal framework solved data security and privacy challenges in cloud in the selected countries.

Besides, comparative research method involved comparing different jurisdictions to establish a conclusion about them.[77] The rationale for using this methodology was to get insights into other country's law, the law of our own country; and in particular, to get a glimpse of our own perceptions and instincts in relation to the law.[78]Equally, this methodology was selected because it is regarded a good means of disseminating fresh ideas into a legal system.[79] Similarly, it is a method widely used to align the laws applied in different legal systems.

Moreover, it helped in to making comparative analysis of the status of security and privacy of personal data in the cloud accorded between Tanzania and South Africa. The researcher checked the availability of specific legislation for security and privacy of data in the cloud. The finding would enlighten the necessity to enact such a legislation. This is because the extent of implementation might not be the same between the two states, as some might have put initiatives worth following and emulating by the other.

[77]Richardson, H., Characteristics of a Comparative Research Design, 2018. Accessed from http://www.classroom.synonym.com/charasteristics-comparative-research-design-8274567.html, on 31st July 2019.

[78]Eberle, E,. J., *The Method and Role of Comparative Law*, Washington University Global Studies Law Review, Vol 8, number 3, 2009.

[79]Vibhute, K., &Aynalem, F., Legal research Methods, Teaching Material prepared under the sponsorship of the Justice and Legal System Research Institute, Ethiopia, 2009. Accessed from http://www.files.Zchilot.wordpress.com, on 31st July 2019.

Additionally, comparative analysis enabled the investigation of European Union (EU) forgetting some insights on how it deals with security and privacy issues in the cloud. EU was selected because its legislation in data protection is regarded as the key point of departure for the development of national data privacy regimes in different parts of the world as well as the best practice.[80]Article 25 of the EU Data Protection Directive, which is now repealed, to a great extent has influenced the international character of data privacy law by imposing a condition to non-EU nations to implement mechanisms that would be considered adequate by the EU for the protection of privacy, if such nations were to continue receiving personal data originating from EU. Similarly, the General Data Protection Regulation retains the adequacy requirement. Consequently, it was deemed imperative to engage in a comparative legal analysis.

1.7 Scope of the Study

This study confined to Tanzania and South Africa. South Africa was chosen due to the fact that it was being named as one of the leading countries in the use of cloud computing in sub Saharan Africa.[81] It was thus found interesting to examine how data security and privacy protection was accorded to the cloud computing environment in the legal regimes of one of the leading countries in implementing and adopting cloud computing. Furthermore, the presence of information security Act known as the Protection of Personal Information Act, 2013 (POPI) was among the reasons for selecting of South Africa. The availability of literature in English and online legal materials was also among the reasons for selecting South Africa as a case study.

---

[80]Bygrave, L. A., Data Privacy Law- An International Perspective, 1st Edition, Oxford University Press.United Kingdom, 2014.

[81]Omwansa. Note 71, supra.

Tanzania was selected because it was the second biggest economy in East African Community (EAC) following Kenya. It is also a country in which cloud computing adoption was growing tremendously. However, the preliminary survey showed that it lacked specific data protection and privacy laws in its legal regime.[82]So, it became of interest to examine how legal frameworks protected data security and privacy in this country without a specific legislation providing for the same. It is however important to highlight that Tanzania was a case study and South Africa served as benchmark for comparative purposes.

1.8 Limitations of the Study

Limitations are constraints and incidences that arise in a study which are largely beyond the researcher's control. They normally limit the extensity to which the study can go. Hence, in most cases, they affect the study outcome and the conclusions that can be drawn.[83]The researcher expected to encounter some limitations while conducting this study. One of them was dearth of literature discussing specifically security and privacy issues in cloud computing in libraries. The second limitation was scarcity of decided cases on privacy and security issues in the cloud, both in Tanzania and south Africa. To some extent, this affected the study. However, all the above limitations are counteracted by opting for the use of online books, online journal

[82]Privacy International & Tanzania Human Right Defenders Coalition., The Right to Privacy in the United Republic of Tanzania, Stakeholders Report, Universal Review, 25th Session in Tanzania, 2015.Accessed from http://www.privacyinternational.org, on 4th January 2017.

[83]Simon, M. K. & Goes, J. Assumptions, Limitations, Delimitations and Scope of the Study in Dissertations and Scholarly Research: Recipes for Success. Seattle, WA: Dissertation Success LLC, 2013. Accessed from http://www.dissertationrecipes.com/wp-content/uploads/ 2011/04/limitationscopedelimitation1.pdf, on 15th January 2017.

articles and other electronic materials from reputable sources. Moreover, the researcher used mainly the cases that tested the constitutional privacy rights to in the study to portray necessity of security and privacy right protection in the cloud.

1.9 Delimitations of the Study

Delimitations of the study are factors that arise from intentional choices that are made when designing the study about where the boundaries of the study are going to be drawn. They mainly arise from the limitations attached to the scope of the study.[84]Privacy and security of data is a wide subject in ICT law. It has many different components, which are difficult to be studied in detail and at once. It is in this line that this study only focused to privacy and security in cloud computing. In spite of the fact that the study used data from developing as well as developed countries, more emphasis was on how developing countries strive to ensure privacy and security of personal data in the cloud. Nevertheless, since there were so many developing countries, the study focused only on Tanzania and South Africa because the researcher found the area interesting for advancing knowledge and shedding light on some legal solutions in the existing problem.

1.10 Organisation of the Study

This study is divided into seven chapters. Chapter One lays out the contextual framework of the study. Chapter Two describes cloud computing concept, its history, evolution and current trends. It also designates what cloud concept means in the field

[84] Wiersma, W., Research Methods in Education: An introduction. Boston, M. A. Allyn and Bacon, 2000.

of communication technologies, its nature and character. Furthermore, it also presents and pronounces some key issues that relate to the negative aspect of cloud computing. Chapter Three covers the description of the theoretical framework of privacy and security. Likewise, it gives an overview of the phenomenon about its background. At the same time, Chapter Four revisits international benchmarks for privacy and security in the cloud environment. It makes an in-depth examination of the engagements for the facilitation of privacy and security of personal data in the cloud, and the extent to which they implicate and enlighten security and privacy in the cloud regulation in Tanzania and South Africa.

Chapters Five and Six respectively discuss the existing legal frameworks as well as practices of privacy and security in the cloud in Tanzania and South Africa. They also discuss the origin, historical background as well as the emerging reforms of privacy and security in the cloud in the above-named countries. These chapters also provide an insight on the extent to which the current legal frameworks address privacy and security issues in the cloud in the context of existing theories and international standards.

Chapter Seven concludes the study and summarises key findings of the study by outlining what has been revealed from the foregoing chapters. It also portrays contribution to knowledge that this study makes as well as the agenda for further research. The main thrust of the preceding chapters includes providing insights in the legal challenges on privacy and security in the cloud in Tanzania and South Africa. It also suggests how both Tanzania and South Africa can devise and craft workable

privacy and security legislation framework suited to their strategic needs and environments.

CHAPTER TWO

ORIGIN AND DEVELOPMENT OF CLOUD COMPUTING

2.1 Introduction

The rise and development of the internet has facilitated the growth and development of different technologies around the globe; cloud computing inclusive.[85] Particularly, from the dawn of early 21st century the evolution of the internet and the prevalent adoption of virtualisation technology[86] has led to the emergency of cloud computing and it has become in the forefront of innovation.[87] Consequently, cloud computing has become one of the concepts which often attracts discussion from all angles, especially the academia and businesses. It is noteworthy that cloud computing model has witnessed a huge move towards its acceptance and adoption by various users and providers over the past few years.[88]

Furthermore, it has been an evolving IT environment, which has remarkably revamped peoples' insight of computing software and its distribution, development models as well as infrastructure.[89]It delivers various utilities as a revolutionary enormous model

[85]Nazir, M., *Cloud Computing: Overview & current Research Challenges*, IOSR Journal of Computer Engineering, 2012. Vol 8, Issue 1, pp. 14-22. Accessed from https://www.researchgate.net/publication/269751258_Cloud_Computing_Overview_Current_Research_Challenges, on 19th April 2018.

[86] Virtualization is a technology that combines or divides computing resources to present one or many operating environments using methodologies like hardware and software partitioning or aggregation, partial or complete machine simulation, emulation, time sharing and others. See Chiueh, S. N. T and Brook, S., (2005) RPE Report, Pp. 1-42. Accessed from http://www.citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.74.371, on 20th Feb 2018.

[87] Kong, et al, note 46. Supra.

[88]Giuseppe A, et al., Provable data possession at untrusted stores. In Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp 598–609. Accessed from http://www.eprint.iacr.org/2007/202.pdf, on 19th April 2018.

[89]Razaque, A., and Rizvi,S., S., *Privacy Preserving Model: A New Scheme for auditing Cloud Stakeholders*. Journal of Cloud Computing: Advances, systems and Applications, 2017. Vol 6, Issue 7, Springer open. Accessed from https://link.springer.com/article10.1186/s13677-017-0076/, on 20th April 2018.

where cloud users can store personal and valuable information remotely and hence avail themselves of on demand prime computer resources.[90] Consequently, it is projected as the upcoming generation of high-tech paradigm for tomorrow's promise.[91] This chapter examines the origin and development of cloud computing. It begins by defining cloud computing from different perspectives. The attention then turns to tracing its origin and development. The description is also used as a springboard for explaining the characteristic, delivery models, and deployment models of cloud computing as developed in literature. Besides, this chapter highlights the dark shortcoming of cloud computing despite its benefits.

2.2 Cloud Computing Concept

Although there is no single universally agreed definition of the term cloud computing, there have been different attempts to define it by various people and organisations. Yousef. *et al* are among the first group, which tried to define cloud computing.[92] According to these scholars, it is a new computing model, which enables manipulators to momentarily exploit computing infrastructures available over the network, which is provided by the cloud service provider as a service on pay per use basis.[93]Particularly, this definition denote to both the computing applications that are provided as services

[90]Peter, M., & Grance, T., *The NIST definition of cloud computin*g cited in Razaque, A.& Rizvi, S., S., note 89, supra.

[91]Buyya, R., et al., *Cloud computing and emerging IT platforms: Vision, Hype, and Reality for Delivering Computing as the 5th utility*. Future Generation Computer Systems, 2009, 25(6):599–616. Accessed from http://www.researchgate.net/publication/2224110211, on 20th April 2018.

[92] Yousef. L., M., et al., Toward a Unified Ontology of Cloud Computing. In Grid Computing Environments Workshop,2008. Accessed from https://pdfs.semanticscholar.org, on 20th April 2018.

[93]Ibid.

over the internet as well as software systems and hardware in the data centres that provide cloud computing services.

Equally, the International Business Machine (IBM) defines it as the distribution or transmission of on demand computing resources.[94] This implies that everything needed from applications to data centres can be accessed over the internet on a pay for use basis.[95] Furthermore, the resources offered are elastic in nature as they can be scaled up or down promptly and simply according to the demand.[96] It is noteworthy that services issued in cloud are also metered so that the client pays only for what he/she uses and the IT resources in the cloud are offered at a self-service mode.[97] It is in the same vein that Lamba and Singh give a simple definition, which provides that cloud computing entails the amalgamation of a technology and platform, which offer hosting as well as storage services over the internet.[98]

Moreover, it is also defined as an environment of the hardware and software resources in the data centres that provide various services over the web or the internet according to the user's requirements or to meet user's needs.[99] Additionally, Kumar and Goudar provide that:

> *"Cloud computing is a complete new technology. It is the development of parallel computing, distributed computing grid, computing, and is the combination and evolution of virtualization, utility computing, Software-as-a-*

[94]IBM, What is Cloud Computing? 2014. Accessed from http://www.ibm.com/cloud/learn/what-is-cloud-computing, on 20th April 2018.
[95]Ibid.
[96]Ibid.
[97]Ibid.
[98]Lamba, H., S., & Singh, G., *Cloud Computing-Future Framework for e-management of NGO's*, International Journal of Advancement in Technology, 2011, Vol 2, No 3. Accessed from https://www.researchgate.net/publication/51917301, on 20th April 2018.
[99]Leavitt, N., "*Is cloud computing really ready for prime time?*" Computer, 2009, vol. 42, no. 1, pp. 15–25, Accessed from https://www.researchgate.net/publication/220477017_Is_Cloud_Computing_Really_Ready_for_Prime_Time, on 20th April 2018.

> *Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).Cloud is a metaphor to describe web as a space where computing has been pre-installed and exist as a service; data, operating systems, applications, storage and processing power exists on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and interactions with service providers."*[100]

However, it is the United States National Institute of Standards and Technology (NIST) that issues a more commonly accepted definition of cloud computing. It defines 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."*[101]

Therefore, from the above explanation, it is established that cloud computing offers expedient on-demand network access to a shared pool of configurable computing resources.[102] Resources in this context denote computing applications, network resources, platforms, software services, virtual servers, and computing infrastructures.[103]In other words, cloud computing can be described as a situation in which computation is delivered by the service provider on subscription basis anytime and anywhere.[104]Still, it is described as a paradigm that enables its consumers as well

---

[100]Kumar, S., &Goudar, R., H., *Cloud Computing- Research Issues, Challenges, Architecture, Platforms and Applications*: *A Survey*. International Journal of Future Computer and Communication, 2012, Vol 1, No 4. Accessed from https://www.academia.edu/7449491, on 20th April 2018.

[101] Mell, P., & Grance, T., A NIST Definition of Cloud Computing. National Institute of Standards and Technology. NIST SP 800–145, 2009. Accessed from http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, on 20th April 20018.

[102] Sun, Y., et al., Data Security and Privacy in cloud Computing, Review Article, International Journal of Distributed Sensor Networks, 2014. pp 1-9. Accessed from http://www.journals.sagepub.com/doi/full/ 10.1155/2014/190903, on 20th April 2018.

[103] Ibid.

[104] Bhowmik, S., Cloud Computing, United Kingdom, Cambridge University Press, 2017.

as businesses to use computing resources which include applications and software in the absence of installation and accessing their data at any computer via internet.[105]

As pointed out, in this part, cloud computing is defined from different perspectives, yet none of the definitions can be considered superior to others on the ground that each has its own limitations. Nevertheless, it is possible to make predilection of a particular definition to suit a particular context. It worth highlighting that this approach is not going to undermine other definitions on the fact that this preference may not fit in other contexts in which other definitions can do. Therefore, in this study, the definition given by the NIST is more preferred than others; and hence it is guiding the study. The rationale for its selection is that it is the commonly accepted definition in defining cloud computing. Further, it is in accord with the gist of this study. Also, it is noteworthy that the term cloud computing is otherwise referred as the cloud, and these terms have been sometimes used interchangeably in this study.

2.3 Emergency and Growth of Cloud Computing

Cloud computing has a long history. Some authors describe cloud computing as the end product of distributed and grid computing.[106] It is an innovation whose emergence can be described in different perspectives: technological and IT deployment perspective.[107] Beginning with technological standpoint, cloud computing is seen as an advancement of computing in which virtualisation technology is used to exploit

[105]Geetu et al, *A Survey on Issues of Security in Cloud Computing*, International Journal of Advanced Research in Computer Science, 2016., Vol 7, No. 6 (Special Issue). Accessed from http://www.ijarcs.info/Ijarcs/article/viewfile, on 24th May 2018.

[106]Ahmed, M & Hossain, M., A., *Cloud Computing and security Issues in the Cloud*. International journal of Network Securities & its Applications (IJNSA), 2014, Vol 6, No 1. Accessed from http://www.airccse.org/nsa/6114nsa03.pdf, on 20th April 2018.

[107]Bohm, M., et al., *Cloud Computing and Computer Evolution*, TechnischeUniversitatMunchen (TUM) Germany, Journal. 2010. Accessed from http://www.researchgate.net>publications, on 27th April 2018.

hardware effectively.[108] Under the IT deployment point of view, cloud computing is regarded as an effort to change the way computing resources and applications are delivered.[109] It is worth highlighting that, in this part, the emergence of cloud computing is described from both perspectives. It begins with the emergency of cluster computing technology, which represents a number of computers engaged to accomplish one task, to improve performance, reduce cost, and enhancing load balancing.[110]

Moreover, due to technological advancement, cluster computing was replaced by grid computing.[111] The latter technology is more disparate, geographically distributed and loosely integrated.[112]The grid computing paved the way for the emergency of utility computing. Under this new model, computing resources are accessed and used from a common pool of resources on pay per use basis or metered service.[113]In addition, the concept of cloud computing traces its origin to the utility computers concept as proposed by John McCarthy in 1961. He proposed that:

> *"If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. ... The computer utility could become the basis of a new and important industry."*[114]

[108]Ibid.
[109] Ibid.
[110]Saravg, A., & Kant, C. *Cloud Computing Security and Privacy Concerns*. International Journal of Information Technology and Knowledge,2012. Volume 5, No. 2, pp. 496-501 Accessed from http://www.csjournal.com/IJITKM/PDF%205-2/56%20Ashis.pdf, on 27th April 2018.
[111] Ibid.
[112]Vitkar, S. *Cloud Based Model for E-Learning in Higher Education*. International Journal of Advanced Engineering Technology, 2012, 3(4), 38-42. Accessed from http://www.pdf.semanticscholar.org/289c/3f3509cec617/fc52905c7b351a3c4c2013.pdf, on 27th April 2018.
[113]Saravg, note 110, supra.
[114]Erl, T., et al., Cloud Computing; Concepts, Technology & Architecture, Service Tech Press, New York.2013.

Ultimately, his ideas matured in 1999 when Salesforce.com became the first company to introduce the concept of distributing enterprise applications by using its website.[115] Cloud computing gained momentum in 2002 when the Amazon Web Service (AWS) was introduced.[116] The AWS platform was a bunch of enterprise designed services that offered computing resources, remotely managed storage, and business functionality.[117]However, it was until 2006 that cloud computing concept appeared in the commercial ground.[118] This was in line with the launching of the Elastic Compute Cloud (EC2) by the Amazon, a service that empowered different companies and organisations to let computing capacity as well as processing power to operate applications in their businesses.[119]When the term was coined in 2007, it generally meant combined hardware and software deployment concept.[120]This was made possible by the introduction of Google Docs, which raised public awareness and spread the news about cloud computing. As of late, introduction of the Google App Engine in 2009, allowed individuals as well as companies to create and store their paper works in the cloud.[121]

2.4 Cloud Computing as a New Medium

The rise and advancement of modern technologies, especially the internet, led to the emergence of cloud computing. However, it developed from the pre-existing and well

[115]Susanto, H., et al, (2012) *A Review of Cloud Computing Evolution Individual and Business Perspective.* SSRN electronic Journal, Volume 4, No. (110)10 Accessed from https://www.researchgate.net/publication/232318287_A_Review_of_Cloud_Computing_Evolution_Individual_and_Business_Perspective, on 29th April 2018.
[116] Ibid.
[117]Erl, note 114, supra.
[118] Ibid.
[119] Ibid.
[120] Bohm, et al, note 109, supra.
[121] Susanto, note 115, supra.

researched concepts including virtualisation, distributed and grid computers.[122] Despite the fact that the concepts underlying cloud computing are not new, the innovation of cloud computing arises from the way it delivers computing services to cloud computing customers.[123]It is now regarded as the future generation paradigm in computation.[124] The use of internet facilitates the delivery of applications and resources as a service in the cloud computing environment.[125]In essence, this new model denotes change from computing as a product that someone can buy to computing which is a service that can be provisioned to as well as accessed by the customer over the web from the cloud.[126] Arguably, it is perceived as the next evolution that is going to have a huge impact on organisations as well as businesses on how they manage their IT infrastructure.[127] It has been accepted as a new computing prototype that can deliver services on demand at a cheaper price.[128]

2.5 Essential Characteristics of Cloud Computing

NIST definition as provided in 2.2 is the most accepted by the industry as well as the academia in defining cloud computing. The NIST model, which is guiding this study establishes five main characteristics of this new paradigm.[129] These characteristics have in the past attracted and are still attracting significant interests from both the

[122] Bohm, et al, note 120, supra.
[123] Ibid.
[124] Sun, et al, note 102, supra.
[125] Ibid.
[126]Kerr, J., & Teng, K.,*Cloud computing: Legal and Privacy Issues*. Journal of Legal Issues and Cases in Business. 2010. Accessed from http://www.aabri.com/manuscripts/111064.pdf, on 8th June 2018.
[127] Ibid.
[128] Ibid.
[129]Caithness, N., et al, *Can Functional Characteristics Useful Define the Cloud Computing Landscape and is the Current Reference Model Correct?* Journal of Cloud Computing: Advances, Systems and Applications, 2017. Accessed from https://link.springer.com/article/10.1186/s13677-017-0084-1, on 30th May 2018.

scholarly research perspectives as well as the industrial perspectives.[130]The characteristics established differentiate cloud computing model from traditional computing and other paradigms.[131] These include on demand self-service, broadband network access, measured services, resource pooling, and rapid elasticity. The characteristics are going to be discussed in detail in subsequent paragraphs.

Initially, on demand self-service is one of the essential characteristics of cloud paradigm. This is the feature which allows the customer to use web services and acquire an additional computer facility, such as server time or network storage, according to his/her needs without long delays and human interference on the provider's side in the process.[132]Moreover, it implies that cloud consumers can define as well as modify computing capabilities, such as server time, quantity of data stored in the cloud and the speed of data access and processing independently according to his needs automatically without requiring human interaction from the service provider.[133]

In addition, it is worth highlighting that cloud computing paradigm calls for the broadband network access. It denotes that resources are accommodated in the cloud and can be accessed through standard devices or platforms such as smart phones,

[130]Sun et al, note 124, supra.
[131] Hofer, C., N., &Karagiannis, G., *Cloud Computing Services: Taxonomy and Comparison*. Journal of International Services Applications, 2011, Vol 2: 81-94. Accessed from http://link.springer.com/article/ 10.1007/s13174-011-0027-x,on 30th May 2018.
[132]Caithness, et al, note 129, supra.
[133]Arutynov, V. V., *Cloud Computing: Its History of Development, Modern State and Future Considerations.* Scientific and Technical Information Processing Journal, 2012, Vol 39, no 3, Pp 173-178, Allerton Press, Inc. Accessed from; https://link.springer.com.article/10.3103/ s0147688212030082, on 30th April 2018.

computers, tablets, laptops, Macs to mention just a few.[134] Putting it differently, it signifies availability of broad network access that can be accessed through different devices or platforms such as mobile phones, computers etc.[135] This is an important characteristic of cloud computing due to the fact that cloud users or customer access cloud services using any device that can connect to the internet, and hence it is regarded as an enabler as well as a trait of cloud computing.[136]

Moreover, measured service is another characteristic of cloud computing. It advocates that service providers are empowered to automatically monitor and record cloud resources spent or allotted to the client so as to facilitate the pay-per-use billing, which is central to the cloud paradigm.[137] This infers that cloud service providers may control, monitor, and optimise the use of cloud computing resources using automated metering tools,[138] resource allocation as well as load balancing.[139] It is noteworthy that cloud clients pay for the resources they used only or what is assigned to them depending on the agreements.

Furthermore, location independent resource pooling is another characteristic of cloud computing. This characteristic is to the effect that computing resources of the cloud

[134]ITU, note 51, supra.
[135]Ibid.
[136]Geetu et al, note 105, supra.
[137]Caithness, note 132, supra.
[138]Cloud Security Alliance, Security guidance for Critical Areas of Focus in Cloud Computing, 2011, Vol 3.0, Accessed from http://www.cloudsecurityalliance.org/csaguide.pdf, on 20th December 2016.
[139]Catteddu, D. & Hogben, G. Cloud Computing Benefits, Risks and Recommendations for Information Security, in Serrao, C., Aquilera Diaz, V., and Cerullo, F., (eds) Web applications Security. IBWAS. Communications in Computer Information Science, 2009, vol 72. Springer, Berlin, Heidelberg. Accessed from http://www.link.springer.com/chapter/10.1007%2F978-3-642-16120-9, on 20th December 2016.

service provider are pooled to serve various clients via multi-tenant model.[140] Through this model, various physical as well as virtual resources are dynamically allocated and reallocated depending on the clients' needs or demand.[141] Notably, location is said to be independent on the sense that the customer has no knowledge or control on the exact site of the provided resources or facilities.[142] However, with the use of the higher level of abstraction the customer may specify the location such as the state, country, or data centre where the resources are located.[143] It is worth highlighting that, that the resources that are referred here include memory, storage, and network bandwidth and processing.[144]This implies that cloud clients share a pool of computing resources with other customers on pay per use basis.[145]

In addition to the above, rapid elasticity is also the characteristics of cloud computing. It is the ability to offer scalable services, which allows automatic quick scaling up or down the resources according to the demand.[146]This implies the ability to adapt to changes of the workload through provisioning and de-provisioning computing resources in an automatic manner to the extent that the available resources match with the demand on that particular time.[147] This allows quick scaling up or down of resources automatically according to the demand.[148]Moreover, through rapid elasticity cloud computing facilitates computing resources as well as client accounts to be

[140]Takabi et al, note 62, supra.
[141] Ibid.
[142] Ibid.
[143] ibid
[144] Ibid.
[145]Caithness, note 137, supra.
[146]Takabi et al, note 144, supra.
[147] Nikolas, H., et al., Elasticity in Cloud Computing: What It Is, and what It Is Not. Proceedings for the 10th International Conference on Autonomic Computing (ICAC, 2013), San Jose, CA, June 24-28.
[148]Takabi et al, note 146, supra.

elastically and rapidly provisioned so as to enable the user to scale their services up or down according to their demand.[149]

2.6 Benefits of Cloud Computing

Cloud computing as a new medium has been around for almost two decades. It has been accepted and adopted by organisations of all sizes and shapes as well as the academia.[150] This is due to the fact that it is coupled with benefits such as cost efficiency, flexibility, almost unlimited storage, automatic software/hardware upgrade, scalability and agility. These are discussed in the following paragraphs.

Adoption and proper implementation of cloud computing has the benefit of cost efficiency to cloud users. According to Reza and his fellow authors, cloud computing is widely adopted on the ground that it helps in reducing cost.[151]By adopting cloud computing, companies and business organisations do not need to invest on hardware and software, as they receive in-house service from the cloud service provider.[152] Cloud customers rent the infrastructure and pay for what they use only. It is noteworthy that it is the service provider who manage, patch, and upgrade cloud services. In this regard, the cloud customer is relieved of the operation and maintenance cost and hence low operation cost.

---

[149]Caithness, note 145, supra.

[150]Attaran, M., *Cloud Computing Technology: Leveraging the Power of Internet to Improve Business Performance*. Journal of International Technology and Information Management: 2017, vol 26: iss,1. Accessed from http://scholarworks.lib.csusb.edu/jitim/vol26/iss1/6, on 220th Dec 2017.

[151]Reza, S., et al, *Cloud computing from SMEs Perspectives: a Survey Investigation*. Journal of Information Technology Management (JITM), 2013, Vol 26, No 1. Accessed from http://jitm.ubalt.edu/xxiv-1/article1.pdf, on 2nd June 2018.

[152]Xue, C., T., S., & Xin, F., T., W., *Benefits and Challenges of the Adoption of Cloud Computing in Business*. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2016, vol 6, No 6. Accessed from http://www.researchgate.net/publication/311972358 _Benefits_and_challenges_of_the_Adoption_of_Cloud_Computing_in_Business, on 3rd June 2018.

Similarly, adoption of cloud computing enhances flexibility in business. With cloud computing, workers become more flexible in and out of the working stations as they can access work related files and other documents from anywhere, all the time and simultaneously.[153] Moreover, they are able to access files from internet through web-enabled devices such as smart phones, notebooks, laptops, and many more.[154] Notably, the services offered by cloud computing increase business flexibility as they enable companies to handle business demand, as the files and the data stored virtually on the internet can be easily accessible and worked upon.[155]

Correspondingly, cloud adoption is coupled with the advantage of automatic software as well as hardware upgrade. This is made possible by the cloud computing feature which allows frequent, safe software updates.[156]This guarantees the best software without disturbing the working schedule.[157]Moreover, the frequent updates do not need prolonged installation of software. This feature does not only lower the cost significantly but also increases profit and put the organisation in technological forefront.[158]

Scalability is another key benefit of cloud computing adoption. With cloud computing, the cloud consumer is able to scale up or down the IT resources according to their

[153] Attaran, note 150. supra.
[154]Xue, note 152. Supra.
[155]Abdulaziz, A., *Cloud Computing for Increased business Value*. International journal of business and Social Science, 2012, Vol 3, No, 1. Accessed from http://www.ijbssnet.com/journals/vol_3_No_1_January 2012, on 5th May 2018.
[156]Xue, note 154, supra.
[157] Ibid.
[158]Abdulaziz, note 155, supra.

needs. It implies that the computing resources can be adjusted to adapt the changes in the work to be done. As a result, the existing resource becomes proportional to the demand at that point of time.[159]It is worth highlighting that scalability feature is automated with the adoption of cloud computing. Moreover, cloud computing is embedded with almost unlimited storage. This is due to the fact that adoption of cloud computing allows the cloud customer to store data in the cloud and hence worry not about running out of storage space or the cost of installing more storage space.[160]

2.7 Cloud Delivery Models

Cloud computing architecture is also categorised basing on service delivery models. Generally, there are different models such as Software as a Service (SaaS), Network as a Service (NaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Storage as a Service and Testing as a Service, to mention just a few. However, this study focuses on the delivery modes extracted from the NIST definition as discussed in part 2.2 above. It establishes three cloud delivery modes, i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).[161] These are discussed in the following paragraphs. SaaS is a cloud computing delivery model in which software and other applications as well as computational resources needed to run them are provided as a service over the internet on demand.[162] The model enables the consumer to use the providers' applications and software that are available in the

[159] Nikolas, note 147, supra.
[160]Abdulaziz, note 158, supra.
[161] Kumar, K. V. K. M. *Software as a Service for Efficient Cloud Computing*. International Journal of Research in Engineering and Technology, 2014, Vol 3, Issue 1. Accessed from http://www.researchgate.net/publication/273302034_SOFTWARE_AS_A_SERVICE_FOR_EFFICIENT_CLOUD_COMPUTING, accessed on 2nd June 2018.
[162] Ibid.

cloud according to his demand.[163] Google App and Sales force are examples of SaaS providers.[164]

In most cases, the consumer use software from different cloud service providers without dealing with deployment and maintenance of the software.[165]Cloud computing customers can access the SaaS (hosted applications) such as Google doc and Gmail from a variety of devices including cell phones, laptops and iPads to mention just a few.[166]In a SaaS model, the service provider is the one who is responsible with assuring security, performance, and availability of the software and applications.[167]However, this model poses privacy and security challenges because the consumer has no control on how input data are processed in the cloud by the service provider.

The PaaS is another cloud computing delivery model in which platform access is offered as a service.[168]The model delivers development platforms and environments for which development tools are hosted in the cloud and the same are accessed through the browser.[169] With this model, customers may set up web applications and services

[163]Turahi, note 65, supra.
[164]Ibid.
[165] Kumar, note 162, supra.
[166]Youssef. A. E. *Exploring Cloud Computing Services and Applications*. Journal of emerging Trends in computing and Information Sciences, 2012, Vol 3, No 6. Accessed from http://www.citeseerx.ist.psu.edu/viewdoc/download.pdf, on 2nd June 2018.
[167] Nazir, M., *Cloud Computing: Overview & Current Research Challenges*. OISR Journal of Computer Engineering (OISR-JRE), 2012, Vol. 8 Issue 1. Accessed from http://www.iosrjournals.org, on 2nd June 2018.
[168]The White Paper -TWP. "Introduction to Cloud Computing". 2010. Accessed from http://www.thinkgrid.com/docs/computing-whitepaper.pdf, 0n 10th June 2018.
[169]Chavan, P., & Kulkarni, G., *Paas Cloud*. International Journal of Computer Science and Information Security (IJCSIS), 2013. Volume 1, Issue 1, Accessed from http://www.irocsjournals.org, on 1oth June 2018.

over the web in the absence of installation of any tools in their computers.[170]This implies that with the purchased access, the customers are enabled to develop and deploy their applications as well as software in the cloud without specialised system administration knowledge.[171]

Rodero, *et al.*, provide a simplified definition of PaaS, as a container platform as well as an execution setting where customers who are developers deploy and run their applications.[172] It is also regarded as execution environment in which third parties who are developers employ and operate other complementary components, which enable the development, testing as well as management of other software components.[173] The model enables customers to build software application employing tools provided by the Cloud Service Provider (CSP).[174] Examples of services offered by the PaaS delivery model to its users include but not limited to tools for designing and development, hosting, support, storage, server software, operating system, scripting environment, architecture, and the overall infrastructure supporting application development.[175] Under this model, customers or developers need not manage and control the basic infrastructure due to the fact that they are managed by the platform automatically.[176] It is worth noting that those resources include but are not limited to

[170] Ibid.
[171]Rouse, M. Platform as a Service (PaaS), 2016. Accessed from http://www.searchcloudcompting. techtarget.com, on 22nd June 2018.
[172]Rodero, L. et al, Building safe PaaS Clouds: A Survey on Security in Multitenant Software Platforms. [Research Report] RR 7838. INRIA, 2011. Accessed from https://hal.inria.fr/hal-00657306, on 22nd June 2018.
[173]Giessmann, A., & Stanoevska, K.,Platform as a Service- A Conjoint Study on Consumers" Preferences, a paper submitted in 33rd International Conference on Information systems, (ICIS 2012) Orlando. Accessed from https://www.alexandria.unisg.ch/publications/218326, on 15th June 2018.
[174] Ibid.
[175] Ibid.
[176]Ibid.

servers, storage, network and the operating system. Google application engine is one of the examples of the PaaS that is provided to end users.[177]

Besides, IaaS is the third cloud delivery model, which is generally regarded as a bottom layer or the footing of cloud computing. It is a model in which the CSP supply a bundle of virtualised computer resources such as a service. These include storage capacity, servers, networking, memory processing power, and bandwidth in the cloud.[178] The customers acquire the resources and employ it to run their operating system.[179] Under this model, the customers outsource their data in lieu of purchasing and installing the computing resources required.[180] The IaaS customers are the ones responsible for running and maintaining of the software applications as well as the operating systems, but they need not manage the basic cloud infrastructure.[181]Some popular examples of the IaaS include Drop box, Microsoft window server and Amazon EC2 web services.[182]

[177]Kumar, S., & Goudar, R., H., *Cloud computing – Research Issues, Challenges, Architecture, Platforms and Application: a Survey*. International journal of Future Computer and Communication, 2012, Vol 1, No 4. Accessed from https://www.ijfcc.org>papers/95-F0048.pdf, on 23rd June 2018.

[178]Yousef, note 166, supra.

[179]Sriram, I. & Hosseini A., Research Agenda in Cloud Technologies, A paper submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010. Accessed from https://arxiv.org/abs/1001.3259?context=cs, on 23rd June 2018.

[180] Iqbal, S., et al, *Service Delivery Models of Cloud Computing: Security Issues and Open Challenges*. Security and Communication Network Journal, 2016, Volume 9, Issue 17, Wiley online Library. Accessed from https://doi.org/10.1002/sec.1585, on 23rd June 2018.

[181] Qi, H., et al, *Sierpinski Triangle Based Data Centre Architecture in Cloud Computing*. The Journal of Supercomputing: 2014, 69(2) 887-907. Accessed from https://www.researchgate.net/publication/261993096_Sierpinski_triangle_based_data_centre_architecture_in_cloud_computing, on 23rd June 2018.

[182]Robert, M., Infrastructure as a Service, Options in Cloud Computing, 2016. Accessed from, http://www.computerweekly.com, on 22nd June 2018.

2.8 Cloud Deployment Models

Correspondingly, in order to deliver cloud computing services, the CSP generally uses different deployment models. According to Kaur, there are four main deployment models in delivering cloud services.[183]These are private cloud, public cloud, community cloud and hybrid cloud. Generally, the main characteristic of cloud computing is that all these models are deployed through the internet via pay as you go policy. A brief description of the deployment models is given below.

Private cloud is a deployment model of cloud computing which provides cloud services to a particular private organisation only, it may comprise a number of consumers.[184]It can be operated, supervised, and owned by the organisation itself, a third-party organisation or jointly run by them either on site or off-site.[185] The main feature of this model is that it involves a well-defined and certain cloud environment in which only the designated client can operate.[186]Under this model, computing resources (the cloud)are accessible and used by a single organisation privately.[187] This enhances reliability, performance, control as well as privacy and security. This is due to the fact that all the data are stored in the organisation's private servers.[188]Yet, like other deployment models, it can be scaled up and down quickly depending on the resources available and the needs of the consumer.[189]

---

[183]Kaur, K., *AReview of Cloud Computing Services Models*. International Journal of Computer Applications, 2016, Volume 140, No 7. Accessed from http://www.ijcaonline.org/archives/volume140/number7, on 24 June 2018.
[184] Ibid.
[185] Ibid.
[186] Rao, C., et al, *Cloud: Computing Services and Deployment Models.* International Journal of Engineering and Computer Science, 2013, Volume 2 Issue 12, 3389-3392. Accessed from http://www.ijecs.in/index.php/ijecs/article/download/2254/2079, on 24th June 2018.
[187] Ibid.
[188] Kaur, note 185, supra.
[189] Ibid.

Moreover, public cloud is another deployment model of cloud computing. It entails provision of cloud infrastructure to the public users over the internet.[190] Under this model, anyone with internet connection can access the resources in proportion to his demand.[191] Similarly, it is a model in which the infrastructure is located offsite in providers' premise and is fully owned by him is enabled to scale up it up and down easily.[192]It is the service provider who is responsible for managing and operating the resources.[193] The model may be provided freely or as a pay as you go service.[194] The model enhances economies of scale, because the customer does not need to set up any resources in advance. That is, they just utilise the resources from the public cloud by using network connection when the need arises.[195] Examples of public clouds include Google App Engine, Amazon Elastic-Compute-Cloud, iCloud, and IBMs blue Cloud to mention just a few.[196]

Community cloud is another type of deployment mode in which cloud infrastructure is provided solely for the use by a particular community of clients that have shared concerns.[197]Under this deployment model, various cloud models are joined together to meet particular requirements of the community of clients.[198] The community

[190] Ibid.
[191] Ibid.
[192] Sen, J., Security and Privacy Issues in Cloud computing, in Ruiz-Martinez, et al (eds) Architectures and Protocols for Secure Information Technology, IGI- Global Publishers, USA, 2013, pp 1-45.
[193] Ibid.
[194] Kaur, note 191, supra.
[195] Ibid.
[196] Sen, note 193, supra.
[197]Rani, D., & Ranjan, R., K., *A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing*. International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Volume 4, Issue 6. Accessed from https://www.ijarcsse.com, on 27th June 2018.
[198] Pal, D., et al., *Cloud computing: A Paradigm Shift in IT Infrastructure*. CSI journal of Computing, 2015, Volume 38, Issue 10. Accessed from https://www.researchgate.net/publication/271644546_Cloud_Computing_A_Paradigm_shift_in_IT_Infrastructure, on 27th June 2018.

members, generally, have and share cloud requirements and concerns such as privacy, security, compliance considerations as well as performance.[199] It may be administered, owned, and controlled by a third part or one or more organisations in the community and the infrastructure may exist off site or on site.[200] This is a type of cloud is preferred by government organisations.[201]An example of community cloud is government cloud (G-cloud).[202]

Lastly the hybrid cloud is a type of cloud in which two or more types of cloud infrastructure such as public and private are amalgamated. They are bound together by standardised or proprietary technology that allows data and application portability and manipulation. Data stored in the private cloud of travel agency by a program run in the public cloud is an example of hybrid cloud.[203]

2.9 The Shortcomings of Cloud Computing

Currently, the world is rejoicing on the advantages brought by cloud computing in business and cooperate world. However, these advantages are not pain free. Even though the cloud unleashes wealth of benefits to business and establishments such as economies of scale, scalability services, on demand network access and location independent resource pooling and many more, it also offers cyber criminals a conducive attacking environment. This is due to the fact that huge amount of data is stored in the same place and at the same time can be accessed on shared resources

[199]Malhotra, R., & Jain, P., *How to Choose an Economic Cloud Deployment Model*. International Journal of Computer and Technology (IJCTT), 2013, Vol 4, Issue 8. Accessed from https://www.ijctjournal.org, on 27th June 2018.
[200] Ibid.
[201] Sen, note 196, supra.
[202] Ibid.
[203]Xue, note 157, supra.

using different devices and users. This implies that there are limitations in cloud computing.[204]These includes invasion of privacy, security challenges and service traffic hijacking to mention just a few. The limitations are discussed in detail in the following subsections.

2.9.1 Invasion of Privacy and Security

As it has been pointed earlier, cloud computing brings vast potentials to the governments, individuals as well as businesses. Nonetheless, it brings with it a pressing concern on invasion of privacy.[205] According to Open Web Application Security Project (OWASP), privacy protection is one of the top ten challenges in the cloud environment.[206] It is worth highlighting that cloud computing model does not necessarily violate privacy. Nevertheless, it is the transfer, the storage, and processing of personal data in the cloud that constitute risks to privacy. This is because users do not have control on how and when their personal data can be accessed, but the cloud service providers.[207]

Consequently, they are able to infringe security and privacy rights of the data subjects by collecting, storing and/or processing personal information without knowledge, consent or authorisation of the data subject, and may arbitrarily censor any type of

[204]Taylor, M., &Matteucci, M.,*Cloud computing*. Computer and Telecommunications Law Review, 2010, 57, 58-9: Laurel Delaney, 10 benefits of Cloud Computing, (Verio) Accessed from https://www.verion.com/resources-centre/articles/cloud-computing-benefitis, on 8th July 2018.

[205] Kong, et al, note 87, supra.

[206] Ibid.

[207]Reeta, S., A., L., et, al., *Implications of Cloud computing for Personal Data Protection and Privacy in the Era of the Cloud: an Indian Perspective*. Law Journal of the Higher School of economics, Annual Review, 2013, pp 64-80. Accessed from https://www.law-journal.hse.ru/2013-Annual%20review, on 8th July 2018.

communication.[208] Moreover, in many cases, the data owner is not aware of where, how, and by whom the data are being processed. In some cases, they may be stored and processed in other countries.[209]

Furthermore, invasion of privacy also entails situations in which sensitive, protected or confidential data stored in the cloud is viewed, used, stolen, copied, or transmitted by a person who is not authorised to do so.[210] It also involves intentional or unintentional release of protected information, which includes personal health information, financial information, personal identifiable information and many others to untrusted environment.[211]A good example of this is the involvement of the Cambridge Analytical in the manipulation of general election in Nigeria in 2007 and 2015; and in Kenya in 2013 and 2017.[212]Personal data of some citizen of these countries were collected from Facebook without their knowledge and used to influence voter's behaviour.[213] Therefore any manipulation of personal data in the cloud without knowledge and consent of the data subject is part and parcel of invasion of privacy and security.

2.9.2 Security Challenges

Security is another issue posed by the coming of cloud computing. While security has various meanings, in this study, it refers to confidentiality, integrity, availability,

[208]De Filippi, P & Belli, L., *Law of the Cloud V Law of the Land: Challenges and Opportunities for Innovation*. European Journal for the Law and Technology, 2012, vol 3, No. 2.
[209] Kong et al, note 206, supra.
[210]Ibid.
[211]Ibid.
[212]Kwamboka, L., After the Face Book-Cambridge Analytical Scandal, can we talk about data Privacy in Africa now? Quarts Africa, April 5, 2018. Accessed from http://www.qz.com/africa/1245876/facebook-cambridge-analytica-scandal-heralds-better-data-privacy-in-nigeria-kenya-other-african-countries, on 31st July 2019.
[213]Ibid.

prevention of unauthorised disclosure, amendment, deletion, and withholding of information.[214] Cloud computing architecture poses security issues on data that is processed and stored in the cloud. As a matter of fact, sensitive data in the cloud, can be accessed anywhere in the globe by anyone.[215] Cloud architecture also attracts malicious hackers as it makes it easy for attackers to hack the cloud system. It is actually for these reasons that the Government of the United States does not store classified data in public cloud.[216]

An, A., Z., et al opine that data theft is a trending issue facing CSPs.[217] In the same vein, Yousef and his fellow authors argue that security in the cloud is one of the main issues which has not received industry wide solution.[218]It has also spawned a plethora of research studies, discussions, speeches as well as policy enactments intending to establish legal and technological solutions to the problem.[219]

2.9.3 Service Traffic Hijacking

Service traffic hijacking is another vulnerability explicably caused by cloud adoption. It is a type of security breach whereby attackers hijack an organisation or individuals

[214]Avizienis, A., et al, Basic Concepts and Taxonomy of dependable and Secure Computing. IEEE Transactions and Dependable and Secure Computing Journal, 2004, Vol 1, no 1, pp 11-33. Accessed from http://www.ieeexplore.ieee.org/document/1335465, on 10th July 2018.

[215]Rajaretnam, T., The Implications of Cloud Computing for Information Privacy: An Australian Perspective. International Journal of Business, Economics and Law, 2014, Vol 5, Issue 4. Accessed from http://www.ijbel.com/wp-content/uploads//2014/12/LAW-7-The-Implication-)f-Cloud-Computing-For-Information-Privacy-An-Australian-Perspective.pdf, on 10th July 2018.

[216]De Fillippi, note 209, supra.

[217]An, Y., Z., Reviews on Security Issues and Challenges in Cloud Computing. A paper presented in IOP Conference Series: Materials Science and Engineering 160 (2016) 012106 doi: 10.1088/1757-899X/160/1/012106, Accessed from http://www.iopscience.iop.org/article/10/1088/1757-899X/160/1/012106, 0n 9th July 2018.

[218]Youseff, note 93, supra.

[219]Robinson, N., et al, The Cloud: Understanding the Security, Privacy and Trust Challenges. A report prepared for Unit F. 5, Director General Information Society and Media, European Commission,2010. Accessed from https://www.rand.org/pubs/technical_reports/TR933.html, on 9th July 2018.

cloud account by stealing safety credentials.[220]The stolen information is then used for doing malicious and unauthorised transactions such as implanting false information, data manipulation, redirecting cloud clients to other illegal sites as well as eavesdropping on different activities and other transactions.[221] An example of this happened in 2010when the Amazon cloud was hacked.[222] As a result, hackers accessed client's information unlawfully and used it to victimize many of the Amazon cloud users.

Moreover, the severity of this vulnerability is clearly shown in Cloud Security Alliance 2013 report in which service traffic hijacking was recognised as the third greatest security risk in cloud computing.[223]Service traffic hijacking can lead to data loss, leakage of personal information, falsification of data, unlawful erasure of data, exposure of data to unauthorised people, and many more data breaches.

2.10 Conclusion

Currently, cloud computing is defined and discussed across ICT industry in different disciplines with differing contexts. To bring the point home, cloud computing refers to a variety of internet-based computing service. It is deployed in different models such as public, private, community, and hybrid models. More so, it is also delivered in different categories such as infrastructure as a service, platform as a service, and

[220]Allouche, g., How Safe is your Cloud Data from Service Traffic Hijacking? 2014. Accessed from https://www.socpub.com/articles/how-safe-is-your-cloud-data-from-service-traffic-hijacking-5653, on 10th July 2018.
[221] Ibid.
[222] Ibid.
[223]Lord, N., A Definition of Cloud Account Hijacking. Digital Guardian, 2018. Accessed from https://digitalguardian.com/blog/what-is-cloud-account-hijacking, on 15th September 2018.

software as a service to mention just a few. Likewise, its peculiar characteristics include on demand self-service, rapid elasticity, measured services, location independent resource pooling and broadband network access and so forth.

Cloud computing is currently the most enticing technology partly due to benefits such as cost reduction, efficiency and scalability. However, it has also a number of disadvantages that raise concerns of the clients in adopting technology. Notably, cloud computing technology entails the use of remote servers and computing resources with huge storage capacity which deprive its users' knowledge of where their information is kept, when and who accesses it. Lack of this knowledge deprive users the control of data and subject their data to manipulation and misuse.

An example of this is clearly shown in the Cambridge analytical scandal previously discussed in 2.9.1. Additionally, some of the cloud deployment models such as the public cloud often experience some forms of malfunction and outrage, which affects the security of data stored in the cloud. For instance, the disruption of the Sales force CRM in 2016 caused storage collapse for more than ten hours. The concern of the present study is the lack of industry-wide solution for these issues and inapplicability of existing laws to some data privacy and security issues in the cloud.

CHAPTER THREE

CONCEPTS AND THEORIES OF PRIVACY AND SECURITY

3.1 Introduction

The concepts of privacy and security have been part and parcel of human history for so many years. As a result, their origins are buried in antiquity.[224]Privacy is an illusory term.[225] It is a sweeping concept that encompasses, among other things, seclusion over one's home, pre-eminence over one's body, one's command over the information about himself/herself, freedom of thought, dispensation from surveillance, protection from searches and interrogation as well as of one's reputation.[226] Due to its nature, it has attracted different theories, which vary in scope over the years.

Of significance to note is that privacy protection cannot be separated from technological development. The rise of computer and development of ICT technologies, for example, have fuelled the concerns in the post-modern society. This chapter presents the concepts and theories of privacy and security, its development and the current position. At this juncture, it is worth highlighting that security concept entails plentiful meanings. It is said to be a combination of features of availability, integrity, confidentiality, which implies the deterrence of the unlawful disclosure of information, averting the unauthorised withholding of information, and last but not least, prevention of amendment or deletion of information.[227] Putting it differently,

[224]Solove, D. J., Nothing to Hide: The False Trade-off between Privacy and Security. Yale University Press, 2011.
[225] Ibid.
[226]Solove, D. J., *Conceptualizing Privacy*. California Law Review, 2002. Vol 90: Pp. 1087-1156. Accessed from http://www.scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2/, on 28th March 2018.
[227] Sun, note 130, supra.

security requires that only the authorised actions are taken against the information.[228]It is noteworthy that security is discussed here as one of the data protection principles, which advocates for reasonable safeguards against risks such as loss, unauthorised access or use, destruction, modification, or disclosure.[229]The rationale is to show the importance of privacy and security in the development of human beings and how it is an issue in cloud computing era.

3.2 Conceptualising Privacy and Security

Privacy and security have slowly and simultaneously developed. It has extensive historical roots in sociological and anthropological debates about how broadly it is appreciated and well-kept-up in various cultures.[230] However, the historical use of the concepts has not been uniform, which brings about misperception about its meaning, scope, and value. Indeed, what is regarded as privacy differs from one society to another; depending on the development level of the society in question, era as well as individuals.[231]

Although, privacy is connected and applied to various social conditions, it has no generally accepted definition of privacy, and it is generally perceived as an imprecise

[228]Avizienis, note 214, supra.

[229] Chang, H., Data Protection Regulation and Cloud computing, in Cheung et al (ed) Privacy and Legal Issues in Cloud computing, Elgar Law, Technology and Society, Cheltenham, UK, 2015.

[230]DeCew, J., Privacy, in Edward N., Z., (ed) the Stanford encyclopaedia of Philosophy, Spring 2018 edition. Accessed from https://plato.stanford.edu/archives/spr2018/entries/privacy/, on 28th March 2018.

[231]Lukacs, A., What is Privacy? *The History and definition of Privacy*, TavasziSzel=spring Wind 2016. Tarulmanykotet, I. kotet, agrartudomany, allam-esjogttudomany, fold-es fizikatudomany, had-es rendeszettudomany. DoktoranduszokOrszagosSzovetsege, Budapest, Magyarorszag, Pp. 256-265, ISB978-615-5586-09-5, accessed from https://www.publication.bibl.u-szeged.hu/10794, on 29th March 2018.

concept.[232] Moore contends that it is very difficult to define the concept of privacy because protocols of association as well as disassociation are guided by culture and are specifically relative.[233]He exemplifies his point by giving an example that opening a door without knocking may be accepted in one culture but considered a grave violation of privacy in another.[234]

In addition, Westin advocates that it is impossible to have a concrete definition of privacy due to the fact that privacy issues are mainly issues of values, power as well as of interest.[235]Westins' concept is supported by Liver, who is of the view that it is difficult to define the notion of privacy, as it is difficult to define other allied services such as equality and liberty.[236] According to her reasoning, privacy is imitative of other concepts such as liberty and equality.[237]The above concepts are in line with Gutwirth's observation that it is difficult to give a precise definition of privacy concept due to the fact that it is not a perceptible item that can be simply enclosed into a definite definition.[238] Wacks cement the above school of thought by arguing that the long quest of privacy meaning has produced an on-going discussion that is often sterile and eventually fruitless.[239]

---

[232]Blume, P., E., Data Protection and Privacy – Basic Concepts in Changing World, in Blume, P., (ed) Scandinavian Studies in Law Volume 56, ICT Legal Issues, Stockholm, Jure Law Books pp 151-164, 2010.

[233]Moore, A., *Defining Privacy*, 39(3) J Social Philos, 2008 411-28, 411.Accessed from https://www.papers.ssrn.com/so13/papers.cfm?abstract_id=1980849, 0n 1st April 2018.

[234] Ibid.

[235] Westin, A., (1995) *Privacy in America. A historical and Socio-political Analysis*. National Privacy and Public Policy Symposium, Hartford, cited in Deighton, (1998) The right to be Let Alone, 12(2) Journal of Interactive Marketing pp 2-4, at p2 .Accessed from https://www.sciencedirect.com/journal/journal-of-interactive-marketing/vol/12/issue/2, on 2nd April 2018.

[236]Liver, A., On Privacy, 2011, p3. Accessed from http://www.alever.net/DOCS/On_privacy_intr.pdf on 20th March 2018.

[237] Ibid.

[238]Gutwirth, S., Privacy and Information Age, Rowman & Littlefield Publishers, Inc, Maryland, 2002.

[239]Wacks, R., The Protection of Privacy, London: Sweet and Maxwell. 1980.

Although privacy concept is difficult to define precisely, some common understanding of privacy still exists. For instance, Warren and Brandeis define privacy as the right to be let alone.[240]On the other hand, Westin defines privacy as the individual's, group's, or institutions' right to control and manage information about them, as well as the right to decide and control when, to what extent and how information about them is communicated to others.[241] Zureik, *et al.* extended Westin's privacy concept by providing six elements of privacy: i.e. the right to be left alone, secrecy, personhood, intimacy, limited access to self and control of personal information.[242]In contrast, Gavison is of the view that privacy is a limitation of others' access to an individual.[243]Moreover, in extending Gavison's view Moore defines privacy as a right to control access to and uses of, places, bodies, and private information.[244]

Indeed, in the widest sense (mainly from the European point of view), privacy is regarded as a fundamental human right, protected in the United Nation Universal Declaration of Human Rights (1948) and subsequently in the European Convention on Human Rights as well as different charters and national constitutions.[245]From early 1970s, the main focus of privacy has been personal information. It was mainly

[240]Warren, S. D., & Brandeis, L. S., *The Right to Privacy*, Harvard Law Review, 1890, 4(5) 193-220, accessed from http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%ATRTP%3E2.0.C0%3B2-C, on 10th February 2018.
[241]Westin, A., Privacy and Freedom, Athenaeum, New York. 1967.
[242]Zureik, E., L.,H., et al surveillance, Privacy, and the globalization of Personal Information: International Comparisons. Montreal: McGill-Queen's University Press. 2010.
[243]Gavison, R., *Privacy and the Limits of the Law*, The Yale Law Journal, 1980, 89 (3) Pp 421-471.
[244]Moore, A., D., Employee Monitoring & Computer Technology: Evaluative Surveillance versus Privacy. Business Ethics Quarterly, 2000. Accessed form https://www.cambridge.org/core/journals/business-ethics-quarterly/article/employee-monitoring-and-computer-technology-evaluative-surveillance-v-privacy, on 4th April 2018.
[245] Pearson, S., & Yee, G., note 10, supra.

intended to protect individuals from government surveillance and probable compulsory disclosure of private information in records.

In 1980s, privacy concerns were associated with telemarketing as well as direct marketing. Well along, attention was given to the growing threat of spamming as well as online identity theft.[246]Different forms of privacy have been identified. These include 'the right to be left alone,'[247], the 'control of information about ourselves,'[248] 'the rights and obligations of individuals and organisations with respect to the gathering, usage, disclosure, and retaining of personal identifiable information'[249] and the emphasis on the ills that arise from privacy abuses.[250]From the above discussion, it is an obvious knowledge that privacy is someone's right to be free from meddling or interference from others. It is of significance to highlight that from the above-mentioned forms of privacy, the gist of this work is informational privacy and security in the cloud. Notably the definition that guides this study is Westin's definition of privacy as the right of an individual, group, or institutions to control and manage their personal information, and the right to control and decide who, when, how and to what extent information about them is shared to others.[251]

Moreover, Pearson defines security as the protection of confidentiality, veracity, and accessibility of information.[252]It is in the same line that Avizienis defines it as the

[246]Ibid, P 7.
[247]Warren, S., & Brandeis, note 240, supra.
[248]Westin, A., note 241, supra.
[249]American Institute of Certified Public Accountants (AICPA) and CICA, Generally accepted privacy principles, 2009. Accessed from http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/downloadabledocuments/gapp_prac_%200909. pdf on 1st March 2018.
[250]Solove, D.J., *A Taxonomy of Privacy*. University of Pennsylvania Law Review, 2006, 154(3), 477, January. Accessed from http:// papers.ssrn.com/sol3/papers? abstract=667622 on 1st March 2018.
[251]Westin, note 248, supra.
[252]Ibid.

combination confidentiality, integrity, availability, deterrence of unauthorised deletion or amendment of information, preclusion of unlawful disclosure of information and prevention of unsanctioned withholding of information.[253] Security is established as one of the essential principles of privacy. It is a principle of privacy which advocates for the measures to protect against unauthorised access or disclosure, destruction, modification and unauthorised use of information.[254]

Privacy concept is sometimes used interchangeably with the concept of security. In Europe, the term privacy is used in relation to data protection laws and regulations. In USA security is used instead of privacy when referring to data privacy laws.[255]The above explanation shows that privacy and security are two sides of the same coin. Nevertheless, there are some distinct differences as well as similarities of the two concepts. Indeed, both terms have a common intention of protecting sensitive data. However, privacy differs from security on the fact that it relates to handling mechanisms for personal information. It deals with individuals' right as well as aspects such as notice, accountability, security, access, choice and fairness of use of personal information.

On the other hand, security is a sub-set of a comprehensive privacy concept. Its main thrust is information privacy as contrary to other forms of privacy such as territorial, matrimonial or bodily privacy. It intends to provide safeguards against security threats such as unauthorised access or use, modification or disclosure and loss of information.

[253]Avizienis, A., et al, note 228, supra.
[254]Kong, et al, note 211, supra.
[255]Pearson, S., & Yee, G., note 245, supra.

The above overview shows that the terms, privacy and security sometimes overlap with each other but they are not the same. For the purpose of this research, privacy concept is used in a broad sense, which includes a range of informational interests in the cloud. Furthermore, security is used as one among the principles or elements of privacy, which advocates for the protection of information in the cloud against loss, unauthorised access and use, destruction, modification and disclosure.

3.3 Origin of Privacy and Development

Privacy right was mostly accepted as the right in 19th and 20th centuries. Nevertheless, it existed long before the time of its acceptance.[256] It is as old as man himself is. It has developed sluggishly throughout the history. Its origin can be traced back to the ancient societies. However, what was considered private and what was accorded legal protection differed.[257] From the legal perspective, the code of Hammurabi[258] is the first code to protect privacy.[259] It contained paragraphs that protected the home against intrusions and the ancient Roman law protected the same.[260] The ancient Hebrew used to have laws that were protecting against surveillance. In England, the off-declared

[256]Lukacs, A., What is Privacy? *The History and definition of Privacy*, TavasziSzel=spring Wind 2016. Tarulmanykotet, I. kotet, agrartudomany, allam-esjogttudomany, fold-es fizikatudomany, had-es rendeszettudomany. DoktoranduszokOrszagosSzovetsege, Budapest, Magyarorszag, Pp. 256-265, ISB978-615-5586-09-5, accessed from https://www.publication.bibl.u-szeged.hu/10794, on 4th April 2018.

[257]Ibid.

[258]The Code of Hammurabi was created in 1780 B. C. E. It is one of the earliest set of laws found and one of the best-preserved examples of this type of document from ancient Mesopotamia. The code is a collection of the legal decision made by Hammurabi during his reign as king of Babylon, inscribed on a Stele. New World Encyclopaedia contributors, (2017) "Code of Hammurabi," *New World Encyclopaedia*, Accessed from, http://www.newworldencyclopedia.org/p/index.php?title=Code_of_Hammurabi&oldid=1003616 , on February 8, 2018).

[259]Solove, note 250, supra.

[260]Ibid.

principles that declared the home as one's castle was made in the 15th century.[261] In English common law, eavesdropping was protected since 1769. English legal scholar defined it as listening "under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[262]

The concept of privacy originated from the difference between private and public.[263] The distinction of these words arises from the natural need of a human being to differentiate himself or herself from all others (Which is as explained above is as old as the man himself).[264] Nonetheless, the perimeter of what is private and what is public differs according to the type of society and time of its existence.[265] Historical records show that members had limited prospects for self-determination as their private lives were controlled and influenced by the state in the ancient societies. Accordingly, Plato, in his writings of the laws dialogue, theorises that the life of the people was indomitable by the state and its aims.[266] This implies that there was no room for individual freedom and autonomy, and everything was done for the sake of public interest. This shows that in ancient societies, the concept of privacy did not exist in contrary to the today's society.[267]

Correspondingly, in the medieval era, privacy was considered a person's right as it is

---

[261]Ibid.

[262]Solove, D. J., & Schwartz, P. M., Information Privacy Law, 16th Edition, New York Wolters Kluwer,2018.

[263]Szabó M. D.Kísérlet A privacy fogalmánakmeghatározására a magyarjogrendszerfogalmaival. InformációsTársadalom 2005, 2, p. 45.

[264]Konvitz, M. R., *Privacy and the Law: a Philosophical Prelude.* Law and Contemporary Problems Journal, 1966, Vol 31, No. 2. p. 272, Accessed from https://www.scholarship.law.duke.edu/lcp/vol31/iss2/3/, on 28th March 2018.

[265]Szabó, note 263, supra.

[266]Bobonich. C., Plato's Laws: a critical Guide. Cambridge University Press, 2011.

[267] Ibid.

the case today. Individuals existed as part and parcel of the community and their private life was largely controlled and monitored by other members of the society.[268] This is evidence that there was lack of individual privacy. However, at the dawn of 19th century, changes in economy transformed the way people lived. Development of economy led to the growth of cities and hence urban life. Urbanisation led to the growth of population in cities and as people were over crowded in cities, they lost privacy as they lived in crowded places. Furthermore, they lost privacy as they were no longer living under close control and watching eye from other members of the community or under the constant moral control set up by them.[269] It is underscored that transformation of the society and the growth of cities provided a fertile ground for the birth of privacy right.

Similarly, the emergency and evolution of (tabloid) newspapers which were a productive ground for gossip and photojournalism facilitated the emergency of privacy right.[270] The consequences of these changes led to the budding of privacy right too.[271]It was Warren and Brandeis who firstly propounded for the privacy threats caused by society as well as technological development in their famous article titled "*the right to privacy*" published in 1890.[272] In their study, they argued that as the society changes economically, politically, and socially, the law has to evolve in the

[268]Lukacs., note 257, supra.
[269]Ibid.
[270]Bratman, B. E., *Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy.* Tennessee Law Review, 2002, Vol. 69. p. 344, accessed from https://www.papers.ssrn.com/sol3/papers, on 10th March 2018.
[271]Simon É. Egy XIX. századi tanulmánymargójára. InformációsTársadalom 2005, 2. p. 36.
[272]Shapiro, F. R. *The Most-Cited Law Review Articles*. California Law Review, 1985, 73(5). 1545. Accessed from https://www.scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2037&context=californialaw review, on 11th March 2018.

same pace to create new rights and hence meet the needs of the society.[273] They were the first to petition the recognition of the right to privacy, which they defined as the right to be left alone.[274] However, it was until the second half of the 20th century when privacy right was accepted and acknowledged in international legal documents.[275] It was accepted as human right and it started appearing in different international and national legislation of the nation's adopting those documents.[276]

3.4 Legal and Classical Theories of Privacy and Security

Privacy is a complex concept with no standard or universally agreed definition.[277] It was accepted as a concept worthy of protection at the end of the 19th century. Its acceptance followed the article titled the Right to Privacy published by Warren and Brandeis in the *Harvard Law Review* at the end of 19th century.[278] Afterwards, due to extensive applicability and intricate nature of privacy, it was theoretically examined in several different manners by different disciplines.[279] This led to the emergence of many theories of privacy from different disciplines such as law, political science, philosophy, medicine, information science, engineering and ethics, to mention just a few.[280] For instance, psychology examines privacy as a mental mechanism that intends to shield and control information.[281] Political science approaches privacy as a public

[273]Warren, note 247, supra.
[274]Prosser, W. *Privacy*. California Law Review Vol. 1960, 48, No. 3. p. 384, Accessed from https://www.scholarship.law.berkeley.edu/carlifonialawreview/vol48/iss3/1/, on 11th March 2018.
[275] Lukacs, note 269, supra.
[276] Ibid.
[277]Pearson, note 255, supra. p. 9.
[278]Shapiro, note 272, supra.
[279]Elder et al., An Empirical Investigation of Privacy: The Impact of the Multiple Levels of Trust, A paper prepared for the American Sociological Association Annual meeting at Kent State University, 2015, accessed from http://www.digitalcommons.kent.edu/cgi/viewcontent.cgi?article=1044&context=research, on 14th March 2018.
[280]Makulilo, note 8, supra.
[281] Elder, note 279, supra.

problem demanding public policy resolution.[282] Philosophy attempts to integrate privacy recondite fundamentals.[283] Furthermore, there have been numerous critical arguments on the concept of privacy or its worth from feminist perceptions and also from philosophical perspectives.[284]

Notwithstanding the presence of many theories, there is a consensus among the advocates of those disciplines that privacy is a concept that is difficult to define, and hence there is no universally accepted definition. Post provides that privacy is a value so multifaceted, so entwined in competing and conflicting, so engorged with numerous and diverse meanings, to the extent that it is difficult to ascertain if it can be clearly addressed at all.[285]In many scholarly writings, this difficulty has been expressed in different ways. It is Professor Daniel Solove who provided a very comprehensive summary of the views emphasised by some dominant researchers in the following paragraph: -

> *"Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy. Arthur Miller has declared that privacy is difficult to define because it is exasperatingly vague and evanescent. According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos. Alan Westin has stated that few values so fundamental to society as privacy have been left so undefined in social theory … William Beaney has noted that even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right. Privacy has a protean capacity to be all things to all lawyers, Tom Gerety has observed. According to Robert Post, privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all. Several theorists have surveyed the interests that the law protects under the rubric of privacy and have concluded that they are distinct*

[282] Ibid.
[283] Ibid.
[284]MacKinnon, C., Towards a Feminist Theory of the state, Cambridge, Harvard University Press, 1989.
[285]Post, R., C., Three Concepts of Privacy. Yale Law School, Faculty Scholarship series, paper 185, 2001. Accessed from http://digitalcommons.yale.edu/fss_papers/185, on 10th March, 2018.

and unrelated. Judith Thompson has even argued that privacy as a concept serves no useful function, for what we call privacy really amounts to a set of other more primary interests."[286]

Furthermore, there are a number of reasons that can be attributed to the difficulties of defining privacy. For example, Gutwirth argues that it is not easy to define privacy because of its abstraction.[287]He is of a view that privacy has several meanings which occur in context; hence, it is a contextual and relative concept.[288] Liver postulates that it is not easy to define privacy concept on the fact that there is difficulty of defining associated values such as equality and liberty.[289] She is of the view that the difficulties of defining privacy arise due to the fact that there are no reasonable conditions that can facilitate the identification of privacy and help in distinguishing it from similar concepts such as equality and liberty.[290] Her arguments provide implication that privacy is a by-product of equality and liberty concepts.[291]

In addition, other reasons or factors that posed a difficulty in defining privacy precisely include but not limited to difference of disciplines from which the scholars belong. In addition, different aspects of privacy due to development of technology and the numerous meanings of privacy and the inherent elusiveness and its contextuality have complicated the task of defining privacy. Last but not least, the acceptance of privacy as a right from different cultures due to development of socio-economic and political factors is another aspect that brings difficulties in defining privacy. These changes

[286]Solove, note 262, supra.
[287]Gutwirth, note 238, supra.
[288] Ibid.
[289]Liver,. Note 236, supra.
[290] Ibid.
[291] ibid

bring about difficulty in defining privacy on the fact that formerly privacy was defined basing on western culture. With new developments, cultures such as those in sub-Saharan Africa, Islamic states, and China have accepted and defined privacy in the context of their history as well as political and socio-economic development.[292]

Despite the absence of a universally agreed definition of privacy, several theories share standards or general features of privacy. Analysts analyse them in different common groups, to enable their understanding as well as upholding a clear focus. For resistance, Moor groups these theories into three groups which are Accessibility Privacy, Decisional Privacy and Informational Privacy.[293]In contrast, Bygrave classifies the theories into four groups: Non-Interference, Limited Accessibility, Information Control as well as Intimacy.[294] The two sets of classification are different in number but some of the contents presented therein overlaps. For example, Moors' information privacy can be equated with Bygrave's information control. Similarly, Moors' decisional privacy is in the same line with Bygrave's Non-interference Theory. However, it is not easy to fit Bygrave's Intimacy Theory in Moors' classification.

Comparable to Moor and Bygrave, Davis classifies privacy into four theories, like Bygrave, but he uses different designation. These are limited Access, Control,

[292]Gutwirth, note 287, supra.
[293]Moor, J., H., *The Ethics of Privacy Protection, Library trends*,1991, 39(1-2) 1991: Intellectual Freedom 69-82. Accessed from http://www.hdl.handle.net/1242/7714, on 10th March 2018.
[294]Bygrave, L., A., *The Place of Privacy in Data Protection Law*, University of Wales Law Journal, 2001, Vol 24, No 1, pp 277-283, at p 282, Accessed from https://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html, at 11th March 2018.

Possession of Information and Leaving Alone.[295]Nevertheless, this classification, to some extent, overlaps with the classification given by Moor and Bygrave. Yet, Davis' classification differs from Moors and Bygrave's on the fact that he includes Possession of Information Theory whereas the latter do not. Additionally, Tavani categorises privacy theories into four groups, as did Bygrave and Davis. Nonetheless, he uses different terminologies such as Non-intrusion, Control, Limitation and Seclusion.[296] It is important to note that though Bygrave, Davis and Tavani's classifications are alike in numbers, they differ in contents. For instance, Bygrave includes intimacy in his classification whereas, Davis and Tavani exclude it. Davis' classifications encompass possession of information while Bygrave and Tavani eliminate it. Similarly, it is difficult to fit in Tavani's Seclusion Theory in Bygrave and Davis' classifications.

Conversely, Whitley organises privacy theories into three categories. These include privacy as Control over Personal Information, Privacy from Judgement or Scrutiny by others, and Privacy as no Access to the Person Ream.[297]The first and the third of Whitley's classification fit in the other classifications mentioned above. However, the second classification falls out of the ambits expounded by other scholars.[298] In contrast, Solove classifies privacy theories into six groups. These are Control over Personal Information, Limited Access to Self, Personal Hood, Secrecy, Intimacy and

[295]Davis, S., *Is there a right to Privacy*? Pacific Philosophical Quarterly, 2009, Vol 9, No 4, pp. 450-475, at p 451. Accessed from https://www.onlinelibrary.wiley.com/doi/abs/10.1111.j.1468-0114.2009.01349, on 15th March 2018.

[296]Tavani, H., T., Philosophical Theories of Privacy: Implication for an Adequate Online Privacy Policy. Metaphilosophy, 2007, Vol 38, No. 1, pp 1-22. Accessed from http://www.onlinelibrary.wiley.com/doi/10.1111/j.1467-9973.2007.00474.x/pdf, on 12th March 2018.

[297]Whitley, E., A., Informational Privacy, Consent and the control of Personal Data; Information Security Technical Report, 2009, Vol 14, No. 3, pp 154-159, at pp 155-156. Accessed from https://www.eprints/se.ac.uk/id/eprint/29030, on 12th March 2018.

[298]These scholars are Moor, Bygrave, Davis and Tavani.

the Right to be Let Alone.[299]However, the above theories as propounded by Solove, seem to override with each other. This is clearly portrayed by Person Hood and Secrecy Theories, which overlaps with the Limited Access to Self and the Right to be Left Alone Theories. The overriding reduces Solove's categorisation of privacy theories into four groups similar to other researchers such as Tavani, Bygrave and Davis.

Similarly, Tavani gives another version of privacy classification with six categories: Restricted Access, Control, Ontological, Categorical, Contextual Integrity and Integrated Theories.[300]Some classes he propound overlaps with other classes provided by others including himself. Moreover, he introduces new theories in the study of privacy, such as Ontological, Categorical, Contextual Integrity and Integrated Theories that are not mentioned by others. It is important to note that though Tavani's new classification is the same in number as Solove's classification, they differ in contents. It is not possible to fit in Tavani's Ontological Theory, Categorical as well as Contextual Integrity in Solove's Theory.

In contrast, Allmer proposes three theories of privacy.[301] These are Structuralist (Restricted Access), Individualistic (Control) as well as Integrative Theories. Allmer's classification, largely, fits in Tavani's classification. However, Tavani's Ontological

[299]Solove, note 286 supra.

[300]Tavani, H., T., Informational Privacy: Concepts, Theories and Controversies, in Himma, K., E., and Tavani, H., T., (Eds) The Handbook of Information and Computer Ethics, Wiley, Hoboken. 2008, Pp. 131-64.

[301]Allmer, T., *A Critical Contribution to Theoretical Foundations of Privacy Studies*. Journal of Information, Communication and Ethics in Society, 2011, Vol 9, Issue 2, pp83-101. Accessed from https://doi.org/10.1108/1477991111148613. 0n 20th March 2018.

Theory as well as Categorical Theory and Contextual Integrity are not part of Allmer's classifications. It is in the same line that Fuchs provides three theories of privacy. These are Restricted Access, Control and Integrative Theories.[302] His classification differs from Allmer's in nomenclature, but they have the same contents. However, Fuchs' classification differs from Tavani not only in contents, but also in number.

As pointed above, the classifications of privacy theories encompass some shared features, regardless of the differences shown. Generally, the theories can be classified into six main categories which are Non-interference, Information Control, Restricted Access, Intimacy, Reductionism and Pragmatism Theories. However, none of them should be regarded as more acceptable or superior than others. This is because all of them are coupled with some limitations. These are discussed in the following part.

3.4.1 Non-interference Theory

The Non-interference Theory is a privacy theory that is also known as Seclusion or Non-Intrusion Theory. It has its origin in the article entitled "The Right to Privacy". It was published by Warren and Brandeis in 1890 in *Harvard Law Review*. In this article, Non-interference Theory was coined as the "Right to be Let Alone".[303] It is against this background that scholars like Solove basically classify this theory as the Right to be Let Alone.[304] Nevertheless, referring to Non-interference Theory of privacy to the right to be alone is too narrow. It excludes other elements or forms of the Non-

[302]Fuchs, C., *Towards an Alternative Concept of Privacy*. Journal of Information, communication and Ethics in society, 2011, Vol 9, Issue:4, pp 220-237, Accessed from https://doi.org/10.1108/14779961111191039, on 20 March 2018.
[303]Warren, S., D., & Brandeis, note 273, supra.
[304]Solove, note 299, supra.

interference Theory which do not precisely denote the Right to be Let Alone. However, for the purpose of this work reference to the Non-interference Theory simply means the Right to be let Alone.

The central idea of the Non-interference Theory of privacy is that a person is considered to enjoy privacy right only if she/he is not interfered with any other person in any way. This implies that an individual is regarded to have privacy or enjoy privacy when there is no one trying to interfere, involve or gain access to him or her. However, according to Moor, Non-interference Theory that is equated to the Right to be Let Alone is too narrow and broad hence does not afford not only a definition but also a comprehensible conception of privacy.[305] It is noteworthy to highlight that this theory of privacy comprises some elements of other theories of privacy such as personhood, control over personal information and access to self.[306]

Different scholars give some criticism to the Non-interference Theory as well as the Right to be Let Alone. For instance, Allen contends that if privacy is regarded as the Right to be Let Alone, any form of aggressive or injurious demeanour directed to another individual could be considered as an abuse of the right to privacy.[307] She argues that if that were the case, then a blow in the nose would be an abuse to personal privacy as good as peeking in the bedroom.[308] Solove attacks the Non-interference

[305]Moor, note 293, supra.
[306]New Zealand ‘s Law Commission, Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1, Study Paper, Wellington, 2008, pp.33-40.
[307]Allen, A., L., (1988) Uneasy Access: Privacy for Women in a Free Society, Rowman &Littlefield, Totowa, NJ, 1988, p. 7.
[308] Ibid.

Theory on the ground that it is too wide and vague conception of privacy.[309] Tavani criticises the Non-interference Theory on the fact that the theory tends to mix the elements or contents of privacy and the right to privacy and hence confusing.[310] He also contends that if privacy simply means the right to be let alone or free from intrusion, then the theory is confusing privacy and liberty.

It is in the same line that Moor criticises the Non-interference Theory on the fact that the right to be let alone is too narrow and too wide at the same time.[311] To support his arguments, he gives an example that if 'A' approaches 'B' on a public road and asks him what time it is, 'A' has not left 'B' alone but neither has 'A' invaded 'B's privacy. Likewise, if without B's consent A goes through B's personal files, then A has invaded B's privacy, but according to this theory A has let B alone. So, it is uncertain on what does the theory intends to protect.[312] Heeney and Weigand provide that the main assumption of Non-interference Theory is that people build their lives in isolation or individually and hence any intrusion from others are a curtailment of the best.[313]

Moreover, they argue that the Non-interference Theory fails to differentiate ordinary human dealings from intrusive ones.[314] However, this appears to be too facile as individuals engage freely in interactions and generally, they demand attention from

[309]Solove, note 304, supra.
[310]Tavani, note 300, supra.
[311]Moor, note 305, supra.
[312]Ibid.
[313]Heeney, C., & Weigand, H., Privacy Protection and Communicative Respect, Proceedings of the 8th International Working conference on the Language-Action Perspective on Communication Modelling (LAP), Tilburg, the Netherlands, 2003, p.3, accessed from http://infolab.uvt.nl/research/lap2003/weigand_heeney.pdf, accessed on 20th March 2018.
[314] Ibid.

others for a pleasing life.[315] Nevertheless, in reality the Non-interference Theory of Privacy or the Right to be Let Alone mislead scholars to think that any kind of information about an individual is a privacy concern. However, if that could be the case, no any type of information about an individual could be collected at all in real life situation.[316] It suffices to say that this is a very important theory in development of privacy in spite of the drawbacks highlighted above. Though it was promulgated ahead of time by Warren and Brandeis in seminal article, it contained some flares of intuition into a stronger theory of privacy.[317] Moreover, the first propounders of the Right to be Let Alone intended to discover the origins of the right to privacy in the common law, not to offer a complete conception of privacy.[318]

3.4.2 Information Control Theory

This is one of the most predominant privacy theories, in which privacy is defined in relation with the control of information.[319] It was originally proposed by Allan Westin in his book entitled *Privacy and Freedom*. He gave a classical definition of privacy as summarised in the following paragraph:

> *"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Viewed in terms of the relation of the individual to social participation privacy is the voluntary and temporary withdraw of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or when among a large group in a condition of anonymity or reserve.*[320]

---

[315] Ibid.
[316] Ibid.
[317] Solove, note 309, supra.
[318] Ibid.
[319] Moor, note 312, supra.
[320] Westin, note 251, supra.

His definition is accepted by many scholars as providing a clear picture of the Information Control Theory. The theory advocates that if a person has control over his personal information, he/she is having privacy.[321] Moreover, it is the theory that is developed upon two assumptions. The first assumption is that a person has power over his/her personal information either directly or indirectly, against data processors as well as data controllers. Secondly, a person has ability to influence the processing of his/her personal information by data controllers and processors directly or indirectly.[322] Here, the term influence and power are basically the same, as the use or exercise of power inevitably encompasses elements of influence.[323]

It is noteworthy that Information Control Theory entails some elements of restricted access.[324] This is supported by the fact that it limits control to the preliminary disclosure of personal information, which shows that the control over personal information originates from the Restricted Access Theory.[325]The theory has also established itself with regards to concealment. The Concealment Theory was put forward by Posner who advocates that someone is enjoying privacy if he can withhold or conceal information about himself.[326] Furthermore, Information Control Theory encompasses some aspects of ownership rights beyond someone's personal information. For example, Parent embraces this right when he defines privacy as the

[321]Wahlstrom, K., & Fairweather, N., B., Privacy Theory of Communicative Action and Technology, 2013. Accessed from http://search.ror.unisa.edu.au/media/researchachive/open /991591017921831/53108686080001831, Accessed on 20th March 2018.
[322]Makulilo, note 280, supra.
[323] Ibid.
[324]Elgesem, D., *The Structure of the rights in Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data, Ethics and information Technology*, 1999, Vol 1, No 4, pp. 283-293. Accessed from https://link.springer.com/article/10.1023%2FA%3A1010076422893, on 21st March 2018.
[325] Ibid.
[326] Posner, R., A., *The right of Privacy*, Georgia Law Review, 1978, Vol 12, No 3, pp 193-422, at p.193.

situation of an individual lack of documented private information about himself or herself known by other people.[327]

The Information Control Theory also perceives privacy as control and self-determination over personal information as well as access to individual's personal affairs.[328] It focuses mainly on personal self-determination than on privacy. The Information Control Theory also embodies some aspects of the Limited Access Theory. Solove appeals for this concept when he provides that control over information can be viewed as a subset of the limited access conception.[329]

Westin defines privacy in relation to individuals as well as groups and institutions. This implies that he had in mind those societies in which groups are central than individuals. Numerous other theorists have supported the Control Theory of Privacy and defined privacy in relation to control of information. It is in the same line that Fried argues that privacy is not merely an absence of information about an individual in the minds of others. Some what it is the control that an individual has upon the information about himself or herself.[330] Miller endorses the Control Theory when he posits that privacy is the person's ability to control the circulation of information about him or her.[331] Beardsley embraces the Control Theory when she describes that privacy

[327]Parent, W., A., *Privacy, Morality and the Law*, Philosophy and Public affairs, 1983, Vol 12, No 4, pp.269-288, at p. 269.
[328]Tavani, note 310, supra. pp.131-64.
[329]Solove, note 317, supra.
[330]Fried, C., *Privacy (a moral analysis*), in Schoeman, F., D., (Ed) Philosophical Dimensions of Privacy, 1984, pp. 203-222. New York: Cambridge University Press.
[331] Miller, A., R., The Assault on Privacy: Computer, Data Banks, and Dossiers, 1971. p.25 cited in Solove, D., J., Conceptualizing Privacy, California Law Review, 2002. Vol 90, No. 4, pp. 1087-1156, at p. 1100.

is an individual's right to decide when and how much information about him or her can be communicated to other people.[332] Schoeman appeals for a version of the Control Theory when he defines privacy as a measure of control over information and intimacies or access.[333]

Although the Control of Information Theory is undoubtedly an element of privacy, it has been criticised by many theorists and a number of objections against it has been raised. Firstly, they argue that the theory underscoring control is wrongly developed and insufficient when it provides that a person loses privacy when he or she has no control over his own private information. For example, Moor states that the definitions that stress control are inadequate because, in some situations, someone may have no control over the transmission of his or her personal information without loss of privacy.[334] Contrarily, the critics suggest that sometimes there can be a loss of privacy without a loss of control and vice versa.[335]Additionally, the proponents of the Information Control Theory are criticised because they did not define clearly the types

[332]Beardsley, E., Privacy: *Autonomy and Selective Disclosure*, in Pennock, J., R., & Chapman, J., W., (Eds.), Nomos XIII: pp. 56-70. New York: Atherton Press,1971.

[333]Schoeman, F., Philosophical Dimension of Privacy: an anthology. Cambridge, MA: Cambridge University Press, 1984.

[334]Moor, note 319, supra. P 75. To highlight his argument Moor, provide examples that, "A can tell B widely known personal information about C in a situation in which C has no control but in which C suffers no loss of privacy. For instance, in normal situations, A can tell B C's name or where C lives or that C likes the Boston Celtics without diminishing C's privacy. Moreover, if control is construed to mean direct, personal control of information, then on the control theory of privacy we are giving up privacy whenever we tell anyone, anything about ourselves if there is no direct control over what the other person will do with the information. This seem at best counterintuitive. For instance, personal information confided to a doctor will be passed on to other doctors and to nurses in normal medical practice beyond a patient's control and yet without any invasion of the patients' privacy. Furthermore, because personal information about us is stored in computer databases, most of us have no control over how that stored information is used. Of course, these data banks are potential threat to privacy if the stored information is improperly released. However, if the information in these databases is properly used or, even more clearly, not used at all, then privacy is not diminished by the simple lack of control over the information. For these reasons the very popular control theory of privacy is not adequate conception of privacy.

[335] Davis, note 295, supra. p 452.

of information that individuals are expected to have control; and the extent of control individuals can expect to have over someone's information.[336] Schoeman provides a good example here:

> *"One difficulty with regarding privacy as a claim or entitlement to determine what information about oneself is to be available to others is that it begs the question about the moral status of privacy. It presumes privacy is something to be protected at the discretion of the individual to whom the information relates".*[337]

From the above observation, it is clearly depicted that according to the Control Theory, individuals can control and protect any information they regard as private and want to control. However, privacy is not merely an issue of individual prerogative, rather, it is dependent on what the society accepts as private and deems apposite to protect.[338]It is in the same line that Whitley while discussing about the challenges of personal control over personal information in an online environment, under the Information Control Theory observes :

> *"Control is seen as something that occurs at the start of a disclosure process and privacy control is seen solely in terms of limiting what personal data is made available to others. In practice however, this is a rather partial view of how personal data is disclosed and shared by others. It is increasingly common for individuals to register with various online services and disclose data about themselves (name, email address, age etc.) This data is then stored in enterprises databases for significant periods of time and may be shared with other parts of the enterprise or selected third party organizations. Whilst in earlier times control over personal data may have been best undertaken by preventing data from being disclosed, in an internet enabled society it is increasingly important to understand how disclosed data is being used and reused and what can be done to control this further use and reuse".*[339]

[336]Solove, note 229, supra.
[337]Schoeman, note 333 supra.
[338]Solove, note 336, supra.
[339]Whitley, note 297, supra.

Hitherto, the above criticism has been contradicted by Shoemaker, who emphasises that the criticism given to the Control Theory seems to be unfair given that the proponents of the Control Theory could provide the extent and ambit of privacy.[340] According to him, it is impossible for the proponents of the Control Theory to provide the extent to which ones' privacy ranges as well as its exact domain of unknown information, and conclude that someone has privacy only when if he can control access to that exact domain of unknown information.[341] Consequently, if there is no unknown information about an individual that is left for him to control, an individual has no privacy either.[342] Yet, the problem of ambiguity still lingers over the Information Control Theory, as there is the need to address precisely what amounts to appropriate zone of information to be controlled and the degree of control needed.[343]

Secondly, Information Control Theory, particularly Westin's version has received criticism for being too narrow. Privacy definition given by Westin stresses that there is a loss of someone's privacy only when something about him has been communicated.[344] However, not all losses of privacy entail communication.[345]A good example of a situation in which there can be loss of privacy without communication of information is given by Davis. He assumes to be naked in his room and Tom peeps through the window.[346] In this scenario, there is the loss of privacy though nothing is communicated because the peeping; Tom knows how Davis looks like when he is

[340]Shoemaker, D., W., Self-Exposure of the Self: informational Privacy and the Presentation of Identity, Ethics and Informational Technology, 2010, Vol 12, No. 1, pp3-15, at p.4.
[341] Ibid.
[342] Ibid.
[343] Ibid.
[344]Davis, note 335, supra.
[345] Ibid.
[346] Ibid.

naked.[347] Similarly, DeCew contends that privacy can be invaded even when no one knows something about one's person, like in situations such as being forced to hear propaganda, being manipulated by subconscious announcements, or being disturbed by an annoyance that frustrates one's capacity to think or read.[348]

Thirdly, the critics of Informational Control Theory criticises that property rights cannot be part and parcel of this theory. For example, Solove observes;

> *"Information can be easily transmitted, and once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously within the minds of millions. This is why intellectual property law protects particular tangible expressions of ideas rather than the underlying ideas themselves. The complexity of personal information is that it is both an expression of the self as well as a set of facts, a historical record of one's behaviour. Further, there are problems with viewing personal information as equivalent to any other commodity. Personal information is often formed in relationships with others, with all parties to that relationship having some claim to that information".*

In other words, property right notions pose a noteworthy challenge when it is extended as part of informational privacy. The challenges extend from the concepts to the principles of owning corporeal properties. Similarly, Moore stresses that if Informational Control Theory entails property rights as well as privacy rights. Then privacy rights may amount to a special form of property right.[349]

Despite the criticism given to the Informational Control Theory, is viewed as an important theory that is directly applicable to privacy issues raised in data processing practices in organisations.[350] It also builds upon and harmonises well with most of the

---

[347] Ibid.
[348] DeCew, J., W., In Pursuit of Privacy: Law Ethics and Rise of Technology. Cornell University Press, Ithaca, New York, 1997, p48.
[349] Moore, note 244, supra.
[350] Bygrave, note 294, supra.

elementary rules of data protection law; especially rules that allow individuals to participate in as well as influencing the processing of their personal data.[351] Additionally, Information Control Theory gives privacy concept considerable standard force, for allowing privacy advocates to tap in its idea of self-determination.[352]

3.4.3 Restricted Access Theory

Restricted Access Theory is a privacy theory that is also known as Limited Access Theory. It is a theory that presupposes that a person has privacy only when there is limited or restricted access over information about him or her in a particular context.[353] There are different theorists with different variants of this theory, who advocate privacy there must be restriction or limitation of access to person or information about the person in some contexts for the sake of privacy. Gavison's variant defines privacy as a limitation or restriction of other's access to a person.[354]According to her, the limitation required for privacy entails three elements that have to work together: anonymity, secrecy, and solitude.[355]

Similarly, Moor defines privacy as a restricted access to an individual or information about that person.[356] He stresses that someone has privacy in a situation if in that situation; information about that person is protected from observation, intrusion as well as surveillance by others.[357]In this context, the term situation is defined to mean

[351] Ibid.
[352] Ibid.
[353] Tavani, note 328, supra.
[354]Gavison, note 243, supra.
[355] Ibid.
[356] Moor, note 334, supra.
[357] Ibid.

an activity in a location, for instance dwelling in one's home. It can also mean relationships like doctor/patient and computer database in which information about individuals is stored.[358] Moreover, Shoemaker defines privacy in terms of limitation or restricted access of someone's information in a certain domain.[359] He sees that the domain of information in which others are having no or limited access to be one's privacy zone.[360]

However, several objections have been raised against the Restricted Access Theory. First, the definition is said to be vague and too broad, regarding the attention given to an individual, any information gained about an individual or any physical access to an individual. This is because if that could be the case then any interference to privacy deprive privacy most of its inherent meaning.[361]Furthermore, its vagueness and broadness is seen on the fact that it does not show what matters are private and what kind of degree of access is accepted as reasonable and which ones amounts to privacy violation.[362] Secondly, Restricted Access Theory underrates the part played by control and choice in privacy. This is to say, it does not consider that in enjoying privacy, one can decide to provide access to one self's information and restrict or deny others that access.[363] Thirdly, it confuses privacy and secrecy, by stressing that an individual has privacy only if access of information about him/her is restricted or limited.[364]

[358] Ibid.
[359]Shoemarker, note 343, supra.
[360] Ibid.
[361]Wacks, R., Personal Information: Privacy and the Law, Oxford University Press, New York. 1993, p 24.
[362] Solove, note 338, supra.
[363] Tavani, note 353, supra.
[364] Ibid.

Nevertheless, Restricted Access Theory has credit for recognizing the importance of having situations, zones or contexts of privacy to restrict or limit outsiders from accessing someone's information.[365] It also gives technology proper credits for enhancing online privacy and the ethical challenges for protecting privacy.[366] It also has some elements of Information Control Theory as well as being compatible with non-interference Theory.[367] The theory also distinguishes privacy from solitude, autonomy as well as liberty.[368]

3.4.4 Intimacy Theory

Intimacy Theory of Privacy defines privacy as a form of intimacy.[369] This is a progressively popular theory, which identifies that privacy is essential for one's self-creation as well as personal relationships.[370] It advocates that privacy is mainly concerned with the sphere of our personal lives that are intimate or sensitive.[371] It also supports that access to some personal information, which is sensitive or intimate, should be restricted.[372] Accordingly, when one's information, which is sensitive or intimate, is divulged, there is a violation of privacy.[373] There are different variants of this theory, yet the most influential one is Inness'. She defines privacy as:

> *"the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions. ",……. an action as intimate if it "draws its meaning and value for the agent from her love, liking, or care" for another person".*[374]

---

[365] Ibid.
[366] Moor, note 358, supra.
[367] Ibid.
[368] Tavani, note 365, supra.
[369] Solove, note 362, supra.
[370] Ibid.
[371] Bygrave, note 350, supra, p 280.
[372] Solove, note 369, supra.
[373] Inness, J., C., Privacy, Intimacy and Isolation Oxford University Press, New York, 1992.
[374] ibid.

The above definition is commendable mainly because it has extended the scope of privacy beyond information and accommodates actions as well.[375] Moreover, it is in the same vein that Gerstein posits that intimacy cannot exist without privacy.[376] Similarly, Fried provides that intimacy is the disclosure of information about personal beliefs, actions or emotions, which an individual does not share with everyone, and has the right not to share.[377] However, his assertion is objected because it defines intimate information as information, which one can choose to reveal to some people, without showing the existing relationship that makes it to be intimate.[378] For instance, an individual may share some information with a priest or lawyer, that he/she may not share with a friend or lover. However, this does not imply that that she/he has intimate relationship with the priest or lawyer.[379]Nonetheless, some criticisms have been generally raised against Intimacy Theory.

First, regardless of the fact that privacy facilitates the development of trust feelings, caring, love and friendship, they do not paint a complete picture of what is generally accorded protection by privacy.[380] DeCew is therefore, on point, when she states that our financial information is private but not intimate.[381]Secondly, objections are raised on the ground that not all intimate or private matters are characterized by friendship,

[375]Makulilo, note 322, supra. p 98.
[376]Gerstein, R., S., Intimacy and privacy, in Schoeman, F. D., (Ed.), Philosophical Dimensions of Privacy, Cambridge University Press, Cambridge, MA, 1984, pp. 265-71.
[377] Fried, C., *Privacy*, Yale Law Journal, 1968, Vol 77, pp.475-493, at pp 484-485.
[378]Makulilo, note 375, supra. p. 98.
[379]Floridi, L., *Four Challenges for a theory of Informational Privacy*; Ethics and Informational Technology Journal, 2006, Vol 8, No.3, pp.109-119, at p.115-116. Accessed from http://www.uhra.herts.ac.uk/bitstream/handle/2299/1816/901128. pdf?sequence=1, on 12th April 2018.
[380] Schoeman, note 337, supra.
[381]DeCew, note 348, supra.

love, trust, and caring. Farber addresses this point when he writes that sexual affairs may exist devoid of caring, liking or love and acts like buying gifts and giving presents are not regarded as intimate but they express friendship, caring, love as well as liking.[382]Thirdly, privacy as intimacy theories is objected on the fact that it fails to acknowledge that the value of privacy is not solely on the growth of intimate relationships. Weinstein observes;

> *"There is a wide range of instances where to speak of something as private is not to imply intimacy. Individuals not intimately related may nevertheless assert that their relation or activity is a private one in the sense that it is not the proper concern of the community or some institution, such as the state, a church, or a business firm".*[383]

The fourth criticism showered to Intimacy Theory is that in some situations intimacy instead of being facilitated by privacy it may suffocate it.[384] An example of this can be seen in small scale societies in which levels of privacy are low while intimacy levels are high.[385] From the above discussion it is clearly depicted that privacy as propounded by Intimacy Theorist, is applicable to modern societies, which are individualistic and found mainly in urban areas.[386]Furthermore, on the other hand, privacy-as-intimacy is regarded too broad, as it does not satisfactorily define the scope of intimacy on the other hand, the theory is viewed too narrow because it excludes other issues that do not encompass loving and caring relationships.[387]

---

[382]Farber, D., A., Book Review: Privacy, Intimacy, and Isolation in Inness, J., C., Constitutional Commentary, 1993, Vol 10, issue 2;510-519. Accessed from University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/166931, on 12th April 2018.

[383]Weinstein,W., L., The Private and the Free: A Conceptual Inquiry, in Ciochon, R., C., Privacy & Personality, 1st Edition, Routledge, New York, 2007.

[384]New Zealand's Law Commission, pg. 39, para 2.31 cited in Makulilo, note 378, supra.

[385]Ibid.

[386]Solove, D., J., Understanding Privacy, Harvard University Press, Cambridge- Massachusetts/ London- England, 2008.

[387] Ibid.

3.4.5 Reductionism Theory

This is a theory that developed as a critic of privacy concept.[388] It is a theory which holds that it is not necessary to have a distinct legal right to privacy.[389] In the legal field reductivism privacy theorists are of the view that claim of the right to privacy can be determined by using other branches of law.[390] In other words, they stress that privacy is a right reducible to other concepts as well as rights, including but not limited to the right to life, liberty, and property.[391] Consequently, it is a superfluous right, which cannot be isolated from its associated rights. The main theorist of this theory is William Prosser, who advances an argument that any privacy claim can be fixed into different tort claims.[392]

Judith Thomson is another prominent advocate of this theory, who asserts that privacy right is not a right on its own, but the one that is overlapping with others, which include the right of being over looked and unlistened.[393] She is trying to reduce or disregard privacy by examining it in terms of a multifarious legal rights as well as non-privacy morals.[394]The variant of privacy put forward by Thomson stresses that privacy right is a cluster of different rights and conceptions, which are not necessarily in common with all rights in the cluster. Hence, there is no need to settle disputes about its

---

[388]DeCew, note 381, Supra.

[389]Peikoff, A., L., *Beyond Reductionism: Reconsidering the right to Privacy*, N. Y. U. Journal of Law & Liberty, 2008, Vol 3, No 1. Accessed from http://www.migration.nyulaw.me/default/files/, on 15April 2018.

[390] Byrne, E., F. Privacy in Chadwick, R., (Ed) encyclopaedia of Applied Ethics, Vol.3, Academic Press, San Diego, CA, 1998, Pp. 649-59.

[391]Peikoff, note 389, supra.

[392] Prosser, note 326, supra.

[393]Thompson, J., J., (1984) the right to Privacy, in Schoeman, F., D., (Ed) Philosophical Dimension of Privacy, cited in Solove, note 386, supra.

[394]Alfino, M. & Mayes, G., R., Reconstructing the Right to Privacy, 2002. Accessed from http://www.csus.edu/.../privacy%stuff/stp%20privacy%20article/privacyformattedforstp.doc, at 16th April 2018.

limitations.[395] However, her variant is objected on the fact that what belongs to a cluster is not clearly established. A different variant of this theory is propounded by David who advocates that if fundamental interests were properly protected, there will be no claim of the right to privacy.[396] He is of the view that claims for the breach of privacy amounts to a fundamental wrong, and the individual's claim to privacy right is derivative, because the state needs to protect the immediate rights.

Some objections have been raised against the Reductionist Theory. Firstly, it is criticised on the ground that it is too broad on the fact that it includes the right not to be listened and looked at in privacy definition.[397]The second criticism raised is that it is too narrow in asserting that privacy is a derivative right. The argument is raised that even if it is a derivative right still, it may form a coherent cluster.[398] So far, it is necessary to highlight that privacy right has some kinds of interconnection with other rights. That is, despite that many national constitutions in the world lack specific provisions for the protection of privacy, the supreme courts in different states are able to glean privacy rights from the provisions of other rights that are specifically provided for in the constitution.

3.4.6 Pragmatism Theory

Pragmatism Theory is a recent theory of defining privacy that is developed by Daniel. J. Solove. He did so after studying and realized the shortcomings of the then existing

[395] Thompson, note 393, supra.
[396] Davis, F., *what do we mean by "Right to Privacy*"? San Diego Law Review, 1959, Vol. 4, p.20 cited in Moore, note 242, Supra.p.413.
[397] New Zealand's Law Commission, note 385, supra.Para 2.5.
[398] Ibid.

theories of privacy. He later labelled them as traditional theories. His new divergent theory is known as a new theory of Privacy or Pragmatism Theory.[399] He is of a view that traditional method of conceptualising privacy eventually comes up short due to the fact that they try to define common group of desirable and appropriate elements which differentiate privacy rights from other categories of rights.[400] He suggests that using a common denominator as a means of conceptualising privacy is wrong.[401] He stresses that privacy is a concept whose meaning cannot be narrowed down to any sole thing. This is due to the fact that it generally stands for a number of associated things.[402] In lieu of the traditional theories, he introduces a new pluralistic approach, which views privacy as a term, which encompasses wide and various groups of associated things.[403]

Pragmatism Theory is propounded by Solove. Borrowing from Ludwig Wittgenstein, he employs the concept of family resemblances.[404] The concept focuses on the interrelated characteristic of a group of things.[405]It accepts that a group of things may not share a core defining characteristic, but may form a network of resemblance which sometimes overlaps and criss-crosses.[406]More so, the result of using the concept is the

[399] Solove, note 386, supra. p.8.
[400] Citron, D. K. & Henry, L. M., *Visionary Pragmatism and the Value of Privacy in the Twenty-one Century*. Michigan Law Review, 2010, Vol 108, pp. 1107-26. Accessed from http://repository.law.umich.edu/mlr/vol108/iss6/15, on 17th April 2018.
[401] Solove, note 399, supra.
[402] Citron, note 400, supra.
[403] Ibid.
[404] Solove, note 401, supra. p, 1091. Wittgenstein's notion of family resemblances suggests that within a family, members share certain characteristics, such as eye color, but not others. Despite some differences, they resemble each other because they draw from the same pool of characteristics.
[405] Sweeney, M., *Book Review on Understanding Privacy by Solove*, D., J., An International Journal of the Information society, 2012, Vol 28, Issue 5, p.1. Accessed from http://doi.org/10.1080/01972243.2012.712488 at 19th April 2018.
[406]Makulilo, note 378, supra. p. 100.

establishment of a principle of a web of relations that will be used to trace and map instead of having principles such as a checklist of conditions that should be fulfilled.[407]

In espousing this concept Solove proposes that it is important to classify certain things as including privacy when it is in resemblance with other things in the same category.[408]In the same line, he promotes a bottom up approach instead of top down approach.[409]More so, the approach he proposes conceptualises privacy founded in particular contexts which evolve all the times.[410] To put it differently, the approach intends to explore privacy contextually. This is by studying particular practices, then assessing if something is private or not, instead of trying to fit every situation into a rigid predetermined category.[411]It is in the same vein that he advocates that in this approach privacy should be looked at in terms of practice.

Additionally, the word practice in this situation denotes activities, traditions, norms and customs.[412]He contends that privacy violations can be studied as interruptions of specific practices such as intrusion on seclusion, meddling with peace of mind, violation of personal security, searches of one's property or person to mention just a few.[413] The importance of the family resemblance model is seen on the fact that the notion of a web of relations is flexible and does not call for stringent boundaries and at the same time does not allow infinite possibility.[414] Besides, Solove stresses that in this approach, the privacy's value should also be examined by relying on context

[407]Sweeney, note 405, supra.
[408] Citron, note 403, supra.
[409] Ibid.
[410] Ibid.
[411] Solove, note 404, supra. p.1093.
[412] Ibid.
[413] Ibid, p.1130.
[414] Sweeney, note 407, supra.

specific basis. This is contrary to using theories, which create an overarching value of privacy such as intimacy, secrecy, or protecting dignity.[415]

Similarly, in his view, privacy value in a certain situation depends on the intention of the practices involved as well as the significance of those purposes.[416] His approach stresses the importance of valuing privacy instrumentally so that it becomes a means of accomplishing other valuable ends.[417]Similarly, Solove observes that landscape of privacy changes regularly to accommodate change in the society, especially with the development of technology. He comments:

> *"….the issue of how we conceptualize privacy is of paramount importance for the Information Age, for we are beset with a number of complex privacy problems, causing great disruption to numerous important practices of high social value."*

However, some objections were showered to Solove's Pragmatism Theory, which he named as a new theory of privacy. Firstly, his concept is objected for being too general such that it overlooks the fact that at some points it is upon the legislature to decide where among other *rights* privacy right fits in.[418]It is noteworthy that the assertion that privacy should be looked at contextually and through practice will enable the lawmakers to solve the problem. Nevertheless, that does not suffice to get the complete picture. They must rely on reasoning from the first principles or the abstract definition of privacy.[419] Therefore, the attempt to conceptualise privacy while negating any other

---

[415] Ibid, p.1145.
[416] Ibid, p. 1144.
[417] Ibid. 1146.
[418]Foye, S., Book Review on Understanding Privacy by Solove, D., J., 2008, Journal of high Technology Law. Accessed from http://www.law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2008-2009/foye.pdf, at 19th November 2018.
[419] Ibid.

theories of privacy rights inexorably, will lead to the vagueness that was hovering over this concept before.[420]This implies that Solove's move of trying to abandon traditional privacy theories is misleading and has a danger of closing the on-going privacy debates.

The second criticism hinges on the ground that the new theory developed allows huge amounts of subjectivity. This is shown by the fact that the community by using this practical-based mode has to agree on what rights privacy surpass and which rights surpass privacy.[421] Moreover, through this concept, it is impossible for people to reach consensus about the value of privacy compared to other rights in different circumstances, as the people are not holding the concept of rights in the same ideological order.[422] Thirdly, the theory as propounded by Solove does not provide the basis for founding the reasons for considering some acts of injury as privacy violations and others are not.[423]

Fourthly, the new theory appears to be a way of theorising privacy violations instead of privacy concept.[424] This is because Solove focuses on the disruption of certain practices which amounts to harm and this attaches itself into legal and policy analysis intended to remedy or prevent harms.[425]Regardless of the objections discussed above, Solove's new theory of privacy as provided in his book of *Understanding Privacy* is

[420]Thierer, A., Book Review: Solove's Understanding Privacy, 2008, The Technology Liberation Front, p. 3. Accessed from http://techliberation.com/2008/11/08/book-review-soloves-understanding-privacy/ on 19th April 2018.
[421]Foye, Note 419, supra.
[422] Ibid.
[423]Makulilo, note 406, supra.
[424] Ibid.
[425] Ibid.

commendable for bringing new light in understanding privacy as well as its importance in the society. It has also done a praiseworthy job in cutting through the muddle that regularly surrounds the concept of privacy.[426]

3.5 Conclusion

Different concepts and theories are being developed on privacy and security discourse due to development of information technology. Consequently, there is no universal agreement with respect to the meaning, scope as well as the ambit of those concepts and theories. Nevertheless, it is important to highlight that certain common understanding is achieved on privacy concepts and theories. Moreover, due to development of information technology, new conflicting theories are emerging and some instead of protecting privacy, affect privacy. The strengths and weaknesses of some of those theories are pointed out above.

Besides, it is important to highlight that regardless of the strength as well as limitations of the privacy theories, it is still plausible to make a preference of a theory that suits the context of this study. The approach is not undermining other theories as the preferred theory ought not to fit well in other particular contexts in which other theories can fit. Therefore, in this thesis the preferred theory is the Restricted Access Theory (or Limited Accessibility Theory). It is deemed appropriate because it is in line with most of the data privacy law principles.

[426] Citron, note 410, supra.

As previously pointed out, the Restricted Access Theory defines privacy in terms of restriction of others' access to a person or information, which presupposes conditions vis-a-vis claims or rights. This is in line with the data privacy law that provide conditions to be met for data processing to be considered lawful. Yet, it is important to point out clearly that other privacy theories also portray privacy with different degrees of limitations. For instance, the Information Control Theory elucidates clearly the concept of consent that is required as a prerequisite for the lawful processing of personal data. Still, in some exception to the general rule, personal data may be processed without the consent of the data subject.

CHAPTER FOUR

INTERNATIONAL BENCHMARKS FOR PRIVACY IN THE CLOUD

4.1 Introduction

Privacy rights used to be protected unilaterally by different nations without due regard to others. Formally, just like other laws and regulations, privacy legislation used to be applicable within the competency and territory of a particular nation only. Nevertheless, in some few instances, national legislation acquired applicability status outside their jurisdiction.[427]However, in a long run, those legislation brought about limitations in transferring of personal data, which led to flimsy protection personal data, isolation as well as economic barriers. To avert and grapple with those challenges, different nations negotiated bilateral agreements, followed by regional and international harmonisation of privacy and data protection legislation as well as policies.[428]As a result, there was a development of regional and international initiatives on personal data and privacy protection, which encompassed substantial co-operation between different countries.[429]

The undertakings led to a rise of agreements that are binding many nations legally as well as politically.[430]It is noteworthy that the internationalisation of privacy as it is understood today originates from European nations since 1980. It was intended to eliminate obstacles in cross border data flow to promote policies and regulations for

[427]Bygrave, L., A., Determining Applicable Law pursuant to European Data Protection Legislation. Computer Law & Security Report, 2000, Vol 16, No 4, pp 252-257, at p 252. He notes that the French Act on Data Protection of 1978, applies to France's remaining overseas Territory, such as Guadalupe.
[428] Makulilo, note 424, supra.
[429] Bygrave, L., A., International Agreements to Protect Personal Data, in Rule, J., B., & Greenleaf, G., (ed) Global Privacy Protection, Edward Elgar Publishing Limited, Cheltenham, UK. 2008, Pp 15-49, at p 16.
[430] Ibid.

international market and guaranteeing its protection.[431]

Thus, regional and international agreements on privacy provide accepted standards for privacy protection laws and as well serving as benchmarks that guide individual countries in drafting domestic laws. Nonetheless, accepted standards for privacy protection that have developed as benchmarks for guiding the drafting and developing domestic privacy laws has its origin in European countries (developed) and hence they may have some limitations in application to developing countries such as Tanzania. This chapter highlights privacy protection law as it is manifested in international law. In this context, international law implies any law, which is binding or non-binding, which is negotiated at international or regional level, and which results in applicability in more than one nation.

In this work, international law is discussed in two categories. First, the discussion begins by briefly looking at the legal and regulatory frameworks that were developed under the patronages of the United Nations (UN). Secondly, the frameworks developed under the auspices of the regional organisations at regional level are also highlighted and discussed. Moreover, general principles of data protection are also explained. Lastly, it is worth noting that the discussion of this chapter forms the bases for the discussion of Chapter Five and Chapter Six, respectively.

[431]Roos, A., (2003) The Law of Data (Privacy)Protection: A Comparative and Theoretical study., LL. D Thesis, UNISA.

4.2 UN Privacy and Data Protection Initiatives

As previously indicated, the current privacy and security protection trace their history back to 1945, the end of the Second World War. That is, most of the international treaties and declarations made under the auspices of the UN for protecting fundamental human rights established the foundation data protection.[432] This part discusses the human right treaties and declarations with the element of protecting privacy as well as the United Nation Guidelines for the Regulation of Computerised Personal Data File (UN Guidelines) which deals with privacy specifically.[433]

The treaties and declarations were negotiated and made as a reaction to the suffering due to the totalitarian oppression before and during the Second World War.[434] It was necessary to protect privacy of information on the ground that the tyrannical regimes relied on the personal data under their authority to earmark and attack humankind.[435]The most noteworthy instruments for this discussion are the Universal Declaration of Human Rights (UDHR) 1948, International Covenant on Civil and Political Rights (ICCPR) 1966 and the United Nation Guidelines for the Regulation of Computerized Personal Data File (UN Guidelines) 1990.

---

[432]Bygrave, note 430, supra.

[433]A/RES/45/95/adopted on 14/12/1990.

[434]Bygrave, L., A., *Privacy Protection in a Global Context- A Comparative Overview*. Scandinavian Studies in Law, 2004, Vol 47, pp.319-348, pp 108-109.

[435]Hilberg investigates the Jews persecution in German under the Nazi regime and perceives the following; "In the hands of the police the identification system together with its personal documents and most importantly the assigned names and the noticeable label in public used to be a strong weapon. Most importantly, the system was a tool for enabling residence and movement restriction. It was also used as a control measure by facilitating picking up of Jews from anywhere and on anytime. It also had a paralyzing effect to the victims, as it made the Jews to be compliant and amenable to the commands that ever. It exposed the Jews and it was like all the eyes were fixed on them. Under those condition, it was impossible for Jews to resist hide or escape, and as a result most of them were lost." Hilberg, R., The Destruction of the European Jew, Holmes & Meier Publishers, New York,1985. Pp 173-180.

Indeed, the Universal Declaration of Human Rights is a landmark document in human rights history.[436]It is the first international declaration of human rights adopted by the General Assembly of the United Nations after the experiences of the Second World War.[437]The declaration establishes the recognition of undertaking basic human rights by the international community.[438] The preamble of the declaration clearly highlights the undertaking particularly in the second, fourth and fifth recitals. It provides;

> *"Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people;……Whereas the peoples of the United Nations have in the charter reaffirmed their faith in fundamental human rights, in the dignity and worthy of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom;….. Whereas member states have pledged themselves to achieve, in cooperation with the united Nations, the promotion of universal respect for and observance of human rights and fundamental freedoms."*[439]

Further, the Universal Declaration of Human Rights is just a declaration of human rights and not a treaty; hence, it does not create legal obligations to the member states directly.[440] Yet, it has been referred to in many judgements in different regional and national courts as the standard source of elementary human rights.[441]Moreover, it has

---

[436]United Nations. The Universal Declaration of human Rights, 2015. Accessed from http://www.un.org/en/universal-declaration-human-rights, on 1st August 2018.

[437]Australian Human Rights Commission. What is the Universal Declaration of Human Rights? Accessed from https://www.humanrights.gov.au/publications/what-iniversal-declaration-human-rights, on 1st August 2018.

[438]Canadian Institute of Health Research (CIHR), Selected International Legal Norms on the Protection of Personal Information in Health Research, 2011. Accessed from www.cihr-irsc.gc.ca/e/document/protection_pi_e_pdf, on 1st August 2018.

[439]United Nations, note 436, supra.

[440]Australian Human Rights Commission, note 437, supra.

[441]O'Donnell, M., K., *New Dirty War Judgements in Argentina: National Courts and Domestic Prosecutions of International Human Rights Violations*. New York University Law Review, 2009, Vol 84, pp 333-374. Accessed from https://www.nyulawreview.org/sites/files/pdf, on 1st August 2018.

a profound impact on the growth of international human rights law.[442]It is noteworthy that regardless of the declaration having no binding force and mechanisms for its enforcement, it is the basis of other different international agreements that are legally binding on the nations which ratify them.[443]

Privacy as a basic human right is explicitly acknowledged under Article 12. The article states, "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, no to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks." However, the language used in the article prohibits only arbitrary interferences to the privacy right, not any other infringements of privacy.[444]Likewise, Article 27 sheds some light on privacy right. Article 27(1) specifically states, "everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits." The expression "freely to participate" as used in the above article connotes principles of consent which is generally a prerequisite in conducting any scientific health research.[445]

Similarly, the International Covenant on Civil and Political Rights (ICCPR) 1966 is another international human rights instrument made under the auspices of the UN. The ICCPR has its basis on the UDHR.[446]It is basically an agreement on civil and political

[442] Ibid.
[443]Ibid.
[444]Canadian Institute of Health Research, note 438, supra.
[445]Makulilo, note 428, supra.
[446]United Nations UN: Human Rights Treaties, Civil and Political Rights, 2014. Accessed from https://www.humanrights.ch/en/standards/un-treaties, on 2nd August 2018.

rights that is legally binding.[447]The gist of the instrument is to implement, give legal effect and clearly elaborate the principles stated in the UDHR.[448]The instrument consists of five recitals as well as fifty-three articles.

The right to privacy is protected in the ICCPR under Article 17. The article provides that:

(1) "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) everyone has the right to the protection of the law against such interference or attacks."

The above provision is worded nearly identical to Article 12 of the UDHR. Yet, in contrast to the former, it prohibits not only arbitrary interference with one's privacy but also unlawful attacks on his honour and reputations.[449]Similarly, the ICCPR does not encompass the limiting clause that is identical to Article 29 of the UDHR.

The state parties are duty-bound to implement the covenant. Furthermore, it is noteworthy that at the international level, the covenant establishes the Human Right Committee (HRC) the covenant while working as complaints handling authority.[450]

[447]Up to 20th May 2014, the general status is that there are only 171 parties to the ICCPR. However only 74 parties signed the treaty. Nevertheless only 69 parties signed and ratified the instrument and five parties have signed, yet they have not ratified the treaty. Accessed from https://www.treaties.un.org/pages/ViewDetails.aspx?chapters=4&clang=_en&mtdsg_noIV-4&src+IND, on 2nd August 2018.

[448]Canadian Institute of Health Research, note 444, supra.

[449]Diggelmann, O., &Cleis, M., N., *How the Right of Privacy Became a Human Right*, 2014. Human Right Law Review, Vol 14, pp 441-458. Accessed from http://academic.oup.com/hrlr/article-abstract/14/3/441/644279, on 2nd August 2018.

[450] ICCPR, Article 28 (1).

The HRC has competent jurisdiction only to the state parties that have declared explicitly to recognise its competency.[451]Moreover, the state party has to ensure that it has invoked and exhausted all the domestic remedies available before submitting complaints to the HRC.[452] If all the attempts to resolve the issue proved failure within six months, the state party is permissible to refer the issue to the HRC.[453]Nevertheless, if the state parties remain dissatisfied after all the efforts of the HRC in resolving the dispute, with prior consent of the state parties concerned, the HRC may assign an ad hoc conciliation commission to determine the dispute.[454]The commission is required to consider the matter, resolve it and issue a report, not later than twelve months after its engagement.[455]In addition, the state parties are required within three months after receiving the report, to notify the chairperson of the committee whether or not they accept the deliberation or contents of the report of the commission.[456]

However, it is interesting and worth noting that the deliberations or comments of the committee based on the complaints submitted carries a huge weight though it is not binding under the international law.[457]The comments, together with the committees' report issued under Article 40 (4) of the ICCPR to the state parties, offer peremptory advice on the purview of the covenant's provision.[458]It is also worth highlighting that the HRC has no qualifications of a judicial body, and hence the enforcement

[451] Ibid, Article 41(1).
[452] Ibid, Article 41(1) (c).
[453] Ibid, Article 41 (1) (b)
[454] Ibid, Article 42 (1) (a).
[455] Ibid, Article 42(7) (a) (b) (c).
[456] Ibid, Article 42 (7)(d).
[457]Ulyashyna, L., Does Case Law Developed by the European Court of Human Rights Pursuant to ECHR Article 8 Add anything Substantial to the Rules and Principles Found in Ordinary Data Protection Principle? A Tutorial Paper Presented at the Norwegian Center for Computers and Law (NRCCL). Spring 2006.
[458]Bygrave, L., A., Data Protection Pursuant to the Right in Human Rights Treaties, International Journal of Law and Information Technology, 1998, vol 6, No 3, pp. 247-284.

mechanism as provided in the ICCPR continues to be comparatively weak.[459] Moreover, the International Court of Justice (ICJ) has no jurisdiction to matters arising from non-observance of the ICCPR, regardless of the fact that the latter is a convention made under the auspices of the UN.[460]It is in this line that jurisdiction on matters provided for in the ICCPR are vested to the national courts of the state parties.[461]

Likewise, the UN Guidelines for the Regulation of Computerised Personal Data files (hereinafter referred as to in the present work as the Regulation)was adopted by the UN General Assembly in December 1990.[462]It represents the initial initiatives by the UN to establish rules and regulations for the protection of personal data.[463]These initiatives by the UN underscored the importance of data protection in the developed community as well as in developing communities in the globe.[464] Unlike the ICCPR and the UDHR, the UN guidelines were made specifically for the protection of personal data.[465]The Council of Europe (CoE) Convention for the Protection of

[459]Ibid.

[460]Crook, J., R.,The International Court of Justice and Human Rights. Northwestern University Journal of International human rights, 2004, vol 1, pp 1-8. Accessed from https://www.law.northewestern.edu/journals/JIHR/v1/2/Crook.pdf, on 4th Aug 2018. See also Article 36 of the State of the international Court of Justice (ICJ/0).

[461] ICCPR, Article 2 (3) (b).

[462]Greenleaf, G., W., Asian Data Privacy Law: Trade and Human Rights Perspective, Oxford University Press, 2014.

[463] The genesis of the UN Guidelines can be traced back to the UN General Assembly Resolution 2450 of December 1968 (Doc E/CN.4/1025) in which the Un Secretary General was invited to scrutinize the effect of technology on human rights, including deliberations of individuals' right to privacy in the light of advances in recording and other techniques. As result of the study a report was published in 1976 asking states to adopt privacy legislations which will provide for computerized personal data systems in the public as well as in private sectors. It should also list minimum standards for such legislations. Bygrave, L., A., International Agreements to Protect Personal Data in Greenleaf, G and Rule, J., B., Global Privacy Protection. The First Generation, Edward Elgar Publishing Limited, Cheltenham, UK/ Northampton, MA, USA, 2008,Pp 15-49, 17.

[464]Weber, R., H., & Heinrich, U., I., Anonymization, Springer, London, Heidelberg. New York, Dordrecht, 2012.

[465]Greenleaf, note 462, supra.

Individuals with Regard to Automatic Processing of Personal Data, 1981[466] (CoE Convention) and the Organisation for Economic Co-operation and Development (OECD), Guidelines on the Protection on Privacy and Trans border Data Flows of Personal Data, 1980[467] (OECD Guidelines) are other regional instruments that preceded and paved the way for the birth of the UN Guidelines.

The essence of UN Guidelines is the first to set out minimum safeguards that needs to be incorporated in domestic legislations of all the member states.[468] Secondly, it meant to guide national and international, governmental and non-governmental organisations when processing personal data.[469]For the above goal of the UN Guidelines to be achieved, it sets out a recommendation of principles to be applicable while processing computerised personal data files. Yet, it is worth noting that the guidelines are mere recommendations, not legal norms binding state parties to it.[470] Moreover, it cannot be overlooked that although the UN guidelines provide for the means of implementation, the duty of developing definite comprehensive regulations and procedures applicable while processing personal data is upon the initiative of each individual state.[471] In doing so, the member states should focus on the principles established in the UN Guidelines as the minimum standards.

[466] ETS No 108, it was opened for signature in January 1981 and it came into force in October 1985.
[467] OECD Document C (80)58/FINAL, adopted on 23rd September 1980.
[468] UN Guidelines, Part A.
[469] Ibid, Part B.
[470]Weber, R., H., & Heinrich, U., I., note 464, supra.
[471] Greenleaf, G., note 465, supra.

The UN guidelines are made up of ten provisions. However, they have neither a preamble nor definitions of terms in the document. The omission weakens the practical usefulness of the guidelines.[472] Furthermore, the application and scope of the UN guidelines are confined to the processing of personal data of an identifiable individual that is held in a computer file in private and public sector.[473] Similarly, the wording of the guidelines provides some exceptions to its applicability. It goes that subject to some appropriate adjustments the principles provided for in the guidelines may also apply to manual files.[474] Correspondingly, in some situations the principles of the guidelines may apply to legal persons in cases where they have information concerning natural persons.[475]

There are seven guarantees or fair information principles for processing computerised personal data set out in the UN guidelines. These include lawful and fair collection, purpose specification, interested personal access, non-discrimination use, accuracy, security, and disclosure limitation (which are linked to purposes specification and interested person principles).[476] These principles are the general personal information principles for processing personal data and they are found in many data privacy instruments in the world.[477]It is worth noting that although they are mentioned and analysed individually, the existence and application of one principle necessitates the presence of the other. This implies that one principle cannot be upheld at the expense of the other.

[472]Bygrave, note 459, supra. p. 30
[473] UN Guidelines, Para 10.
[474] Ibid.
[475] Ibid.
[476]Greenleaf, G., note 471, supra.
[477]Makulilo, A., note 445, supra.

Trans-border data flow is also an important concern of the UN guidelines.[478] It is a requirement of the guidelines that if two or more nations are contemplating of transferring personal data and they are having comparable safeguards for protection in their laws, information should be freely circulated in those jurisdictions. Yet, if there are no reciprocal safeguards, the guidelines provide that limitations to such circulation may not be imposed unduly and only as far as the protection of protection demands. However, the provision raises some questions. The first question is who is duty-bound to ascertain the comparability of safeguards? Second, what are the benchmarks/criteria of comparison? What is the basis that the concerned nations should consider, so that they will not impose unjustifiable restrictions to the free flow of information? The guidelines do not provide answers to those questions. The silence certainly, leads to practical difficulties in the implementation of the guidelines.

Moreover, for these UN guidelines to take effect, UN calls the member states to appoint a regulatory authority to offer supervision.[479]It is in the same line that the guidelines set out three characteristics that are necessary for the regulatory authority.[480]These include technical competence, impartiality, and independence in regard to persons or agencies, which are responsible for establishing as well as processing data.[481]Similarly, the guidelines provide for the powers of the regulatory authority as part and parcel of that implementation. The latter should be empowered to impose criminal sanctions and the power to issue individual remedies when the principles are not adhered to.

---

[478] UN Guidelines, Para 8.
[479] Ibid.
[480] Ibid.
[481] Ibid.

Regardless of the fact that the UN guidelines underscore the importance of data protection in the world, its principles have been underused and undervalued.[482]This is mainly caused by its status of being mere recommendations and hence its implementation being left to the discretion of the member states.[483]As a result, the guidelines have not had a substantial impact since their approval.[484] Since the guidelines came into being, there have been huge technological advances, which qualify to necessitate reform in the privacy instruments.[485]Nevertheless, strangely enough, there is no current attempt to amend the UN guidelines.[486] It looks like the guidelines have been abandoned. However, there is a plausibility for the guidelines to influence security and safety in cloud in future due to the fact that currently privacy is back on the UN agenda as well as in government and international organisations.[487]

The analysis of the UN systems privacy and security protection leads to the following conclusion:

First, while the ICCPR and the UDHR lay down strong normative basis for privacy protection laws, accepted both in regional and state jurisdictions, they do not expressly provide for data protection principles.[488]However, their normativity are clearly depicted in the recitals as well as preambles of the national and regional privacy and data protection legislation. Consequently, this upholds the understanding and

[482]Casagran, C., B., Global Data Protection in the Field of Law Enforcement: An EU Perspective. Routledge, New York, 2017.
[483] Ibid.
[484]Greenleaf, note 476, supra.
[485]Casagran, note 483, supra.
[486] Ibid.
[487] Greenleaf, note 484, supra.
[488]Kuner, C., *An International Legal Framework for Data Protection: Issues and Prospects*. Computer Law & Security Review, 2009, Vol 25, pp, 307-317. Accessed from https://papers.ssrn.com/so13/papers.cfm?abstract_id=1443802, on 5th August 2018.

acceptance of the international instruments pointed our earlier within national legal systems. Likewise, the incorporation of privacy right in the Bill of Rights in many national constitutions is considered to be the domestication of the privacy right as established by the UDHR and the ICCPR.

Secondly, the UN guidelines are the only instrument that deals with data protection specifically under the auspices of the UN. However, the guidelines are mere recommendations, and hence do not legally bind any nation. As a result, the instrument receives little attention compared to other legally binding instruments on privacy and data protection. This implies that under the auspices of the UN, privacy protection is not given its due weight regarding the development of technology such as cloud computing which increases threat to informational privacy and security.

Thirdly, the task of coming up with a truly global legal binding privacy convention or treaty is a dream yet to come true. However, initiatives for creating that kind of instrument are going on and the task of drafting proper rules intended to be applicable internationally is also going on. In addition, regardless of the fact that there is a dire need for the international legal intervention in the field, realistically, there are minimal possibilities of having a convention made under the auspices of the UN being adopted in the near future. This is mainly caused by differences in culture, history as well as legal orientations in relation to data protection.[489]The following part discusses privacy and data protection in regional systems.

[489]Ibid.

4.3 Europe

Europe is the leader and hence at the forefront of privacy and data protection initiatives in the world.[490]Privacy and data protection regimes in Europe are said to be the oldest and more advanced with reference to others.[491] Other scholars regard it as the gold standard in the world.[492]Data protection regimes in Europe grew under the initiatives of three regional organisations, which are the OECD,[493] the Council of Europe[494] and the European Union.[495]Moreover, some of the instruments made under the auspices of

[490]European Union Agency for Fundamental Rights &the Council of Europe, Handbook for European Data Protection Law, 2018 Edition, Luxembourg, 2018.

[491] European Data Protection Supervisor, The History of the General Data Protection Regulation, 2018. Accessed from https://edps.europe.eu/legislation/history-general-data-protection-regulation_en, on 10th August 2018.

[492] Ibid.

[493]OECD is an international Organization for Economic Co-operation and Development. It was established in 1961 with the mission of promoting policies that are going to improve the economic and social wellbeing of the people around the world. Its origin can be traced back to the Organization for European Economic Co-operation (OEEC) that was established in 1948. A cooperation that was formed with the intention of reconstructing a continent ravaged by war. Currently, its' headquarters is in Paris, France. As of 2017 it has 36-member states. These include Australia, Austria, Belgium, Chile, Czech Republic, Canada, Denmark, Finland, Estonia, German, France, Hungary, Iceland, Greece, Ireland, Japan, Italy, Israel, Korea, Mexico, Latvia, Netherlands, Lithuania, Norway, Portugal, Poland, Luxembourg, New Zealand, Slovak Republic, United States, Turkey, Spain, Slovenia, United Kingdom, Switzerland and Sweden. Accessed from https://www.oecd.org/about/membersandpartners/ on 15th August 20198.

[494]Council of Europe is the oldest and the largest of European institutions founded in 1949. It was established with the intentions of achieving greater unity among its members as well as promoting human rights, democracy, cultural co-operation and the rule of law among others. To realize its aims it has adopted more than 200 different treaties and many recommendations and declarations. Yet, it is still adopting others. Its headquarters is in Strasbourg France. It brings together 47-member states. These are Austria, Albania, Armenia, Andorra, Belgium, Bulgaria, Azerbaijan, Bosnia and Herzegovina, Croatia, Cyprus, Estonia, Czech Republic, Finland, Denmark, France, Georgia, German, Greece, Hungary, Italy, Latvia, Liechtenstein, United Kingdom, Ukraine, Turkey, The former Yugoslav Republic of Macedonia, Switzerland, Sweden, Spain, Slovenia, Slovak Republic, Serbia, San Marino, Russian Federation, Portugal, Norway, Romania, Poland, Netherlands, Montenegro, Moldova, Lithuania, Malta, Monaco and Luxembourg. Accessed from https://www.eda.admin.ch/eda/en/home/foreign-policy/international-organizations/council-europe.html, on 15th August 2019.

[495] EU is a supranational and intergovernmental union made up by 28 members states from Europe, created in 1993 following the Maastricht Treaty. The member states share economic as well as political relations. The main focus of the union is to create a single market through a standardized system of laws which are applicable to all member states. It also intends to enable free movement of goods and services, people and capital within the boundaries of all member states. The unions history can be traced back to the aftermath of the second World war, which led to the establishment of cooperation as a way of preventing future wars in Europe. These include European Economic Community (EEC) of 1957 and European Community (EC) in 1967. The EC was renamed in 1992 to become EU and later a treaty was signed in Maastricht in 1993 and hence the birth of EU. Its

the above organisations follow the footsteps of the UDHR and the ICCPR in addressing privacy issues. These instruments include the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ECHR),[496] the Treaty Establishing a Constitution for Europe of 2004[497] and the Charter of Fundamental Rights of the European Union of 2010 (CFR).[498] It is worth noting that in all the above-named instruments, privacy protection issues are not the main concerns, yet they are dealt with remotely.[499] Hitherto, they are important as they provide a firm legal foundation for growth of privacy and data protection law regimes.

Additionally, some agreements stemming from the above-named regional organisations are of more practical importance in determining national laws on privacy and data protection.[500]The noteworthy ones are the OECD guidelines on the Protection of Privacy and Trans-border Data Flows of Personal Data of 1980,[501]the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CoE Convention 108/1981)[502] and Directive 95/46/EC, which is recently repealed with effect from 28th May, 2018 by the EU General Data Protection Regulations (GDPR).Since their coming to force to date the instruments

member states include France, Netherlands, Italy, Belgium, German, Luxembourg, Greece, Denmark, Ireland, United Kingdom, Spain, Portugal, Sweden, Finland, Austria, Croatia, Bulgaria, Cyprus, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovenia, Slovakia, Czech Republic, Estonia. However United Kingdom is not a member any more to the EU. Accessed from https://europarlamentti.info/en/European-union/history/, on 15th August 2018.

[496]The treaty was opened for signature on November 4th, 1950, came into force in September 3rd, 1953. Accessed from https://www.europewatchdog.info/en/international-treaties/convention-on-human-rights/, on 16th August 2018.

[497]O.J. C310/01, 16 December 2004, pp.1-474.

[498]The treat came into force in March 2010.

[499]Makulilo, note 477, supra.

[500] Bygrave, note 472, supra.

[501]OECD Doc. C (80)58/FINAL; adopted 23rd September 1980; hereinafter also termed 'OECD Guidelines'.

[502]ETS No. 108 opened for signature 28th January 1981, in force 1st October 1985; hereinafter also termed 'CoE Convention'.

have greatly influenced non-European nations to adopt privacy as well as data protection regulations in line with the European style. Their impact has also been widely expounded in some influential scholarly works like 'The EU Data Protection Directive: An Engine of a Global Regime.'[503]The European Union Data Privacy Directive and International Relations',[504]The Long Arm of the EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites World Wide?'[505] and 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalizations of Convention 108'.[506]Regardless of the fact that Directive 95/46/EC is repealed, articles that make it to have global impact are incorporated in the GDPR. As a result, the new law obliges non-European nations to adopt privacy and data protection laws and regulations in the European standard.[507]The following section presents contemporary agreements and treaties with regard to security and privacy in cloud.

[503]Birnhack, M., D., *The EU Data Protection Directive: An Engine of a Global Regime*. Computer Law & Security Review, 2008, Vol 24, Issue 6, Pp 508-520. Accessed from https://www.sciencedirect.com/science/article/pii/SO267364908001337, on 16th August 2018.

[504]Salbu, S., R., *The European Union Data Privacy Directive and International Relations.* Vanderbilt Journal of Transnational Law, 2002, Vol 35, Pp 595-655. Accessed from https://www.researchgate.net/publication/23724380_The_European_Union_Data_Privacy_Directive_and_International_relations, on 17th August 2018.

[505]Moerel, L., The *Long Arm of the EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide*? International Data Privacy Law, 2011, Vol 1, Issue 1. Accessed from https://www.academic.oup.com/idpl/article/1/1/28/759646, on 17th 2018.

[506] Greenleaf, G., *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalizations of Convention 108. International Data Privacy Law*, 2012, Vol 2, Issue 2. Accessed from https://papers.ssrn.com/so13/papers.cfm?abstract_id=1960299, on 20th August 2018.

[507] Article 45 of the General Data Protection Regulation, 2016/679. Accessed from https://www.gdpr-info-eu, on 20 August 2018.

4.3.1 Council of Europe Initiatives

The Council of Europe is one of the first international organisations to initiate the practice of regulating privacy so as combat privacy threats raised by development in information technology, particularly the use computer technology.[508]It is the leading international organisation that has drafted a binding multilateral instrument that is specifically regulating the protection of privacy and personal data.[509] In 1981, it adopted Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[510] It entered into force on 1st October 1985.[511] Since 28th January 1981, the Convention 108 is open for signature by the member states as well as accession by non-members. Presently, all 47 member states of the CoE have signed and ratified the treaty.[512] It is also ratified by six non-members of the Council of Europe including four states from Africa.[513]

The history of the Convention 108 can be traced back to late 1960s and early 1970s Councils' resolutions and recommendations. Most important, resolutions espoused by the CoE Ministers Committee. These are Resolution (73)22 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector,[514] and Resolution (74)29 on the Protection of the Privacy of Individual vis-à-vis Electronic

[508]The Council of Europe, note 495, supra.
[509]Bygrave, note 500, supra.
[510]The Convention is also known as Convention 108 or ETS No. 108.
[511]Council of Europe, Details of the Treaty No. 108, 2018. Accessed from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, on 20th September 2018.
[512]Council of Europe, Chart of Signatures and Ratifications of Treaty 108, 2018. Accessed from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=mrQOsyiE, on 3rd October 2018.
[513]These include Cape Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay. Accessed from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=mrQOsyiE, on 3rd October 2018.
[514]Adopted by the Committee of Ministers on 26th September 1973 at the 224th meeting of Ministers' Deputies.

Data Banks in the Public Sector in 1973 and 1974 respectively.[515]The annexes to the resolutions generally comprise comparable sets of principles for personal data protection, drawing motivation from successful countries in that area such as Sweden, Belgium, German, and US legislative initiatives.[516]

There are different reasons that necessitated the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of personal Data. The first one is the gaps that were found in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) 1950.[517] Though the ECHR protected Human Rights and other fundamental rights, it did not provide for protection of privacy of a person when personal data is computer processed, especially in private sector, such as banking and insurance sector.[518]Likewise, most member states of the CoE lacked proper laws for privacy and personal data protection.[519]Apart from the absence of data privacy laws, there was no harmonisation in national laws for enhancing free flow of data across national borders. To combat the above-named challenges, it was found necessary for the CoE to adopt the resolutions embodied with data protection principles.

Primarily, the Convention was envisioned to provide for computerised processing of personal data in private and public sectors, including state security agencies and police as well.[520] The Convention also allows member states in some exceptional situations

[515]Adopted by the Committee of ministers on 20th September 1974 at the 236th meeting of Ministers' Deputies.
[516] Bygrave, note 509, supra.
[517]Hondius, F., W., *Data Law in Europe*, Stanford Journal of International Law, 1980, Vol 16, pp 87-111, at p. 92.
[518]Ibid.
[519] Greenleaf, note 506, supra.
[520]Convention 108, Article 3(1).

to provide in their laws and apply its principles in corporate and collective entities (which are also known as juristic or legal persons).[521]The permit also encompasses personal data processed manually.[522] Moreover, the Convention is flexible enough to allow the member states to provide higher standard of personal data protection to its citizens than it stipulates.[523] It is worth keeping in mind that in contrast with the OECD guidelines, the Convention is an international treaty that is legally binding its members on matters relating to personal data production.

In addition, Convention 108 requires member states to enact domestic laws which incorporate its data protection principles.[524]However, of itself, it does not provide precise package of rights to be directly enforceable in domestic courts.[525]Moreover, it is important to note that while the Convention was intended to be a catalyst and a basis of domestic legislation in member states, it did not want to foil those efforts by dictating a set of rules to be applicable in domestic courts of the member states.[526]

The core of the Convention is found in the second chapter, where the general principles for processing personal data are provided. It provides for eight basic principles, which are identical to the ones promulgated in the OECD Guidelines as well as in laws of different member states. Nevertheless, the fact that they are provided for in the Convention, gives them the status of being a point of reference in questions regarding

[521] Ibid, 3(2), (b).
[522] Ibid, 3(2), (c).
[523] Ibid, 11.
[524] Ibid 4(1).
[525] Explanatory Report, para 38 and 60.
[526]Hondius, F., W., *A Decade of International Data Protection*. Netherlands International Law Review, 1983, Vol 30, issue 2, pp. 103-128. Accessed from https://www.cambridge.org/core/journals/netherlands-international-law-review/article/decade-of-international-data-protection/36B00324DFAA59FAF788B81787D26BE1, on 18th Sept 2018.

these principles at the national as well as international level. In a nutshell, these principles may be discussed as follows:

Fair and lawful processing is the first principle which maintains that personal data should be obtained and processed fairly and lawfully.[527] The principle requires among other, things transparency in processing personal data as well as using the data only for specified purposes known to the data subject prior to the collection. Similarly, it states that processing should as well be authorised by law or consent of the data subject.[528]Purpose specification is the second principle enshrined in the Convention. This principle presupposes that 'personal data shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.'[529] This principle is to the effect that data controllers are prohibited from storing in their custody data without defined and legitimate purposes.[530]Minimalism is the third principle, which advocates that personal data collected and stored should be adequate, relevant, only limited to what is required for attaining the purpose for data collection or storage.[531]

In addition, adequate information quality is the fourth principle. It enunciates that personal data 'shall be adequate, accurate, and relevant in relation to the purpose for

[527]Convention 108, Art 5(a).
[528]Bygrave L., A., *Privacy and Data Protection in an International Perspective*. Scandinavian Studies in Law, 2010, Vol 56, pp 165-200, at p.175. Accessed from http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmarteriale/privacy-and-data-protection-in-international-perspective.pdf, on 20th sept 2018.
[529]Convention 108, Art 5(b).
[530]Explanatory Report, para 41.
[531]Convention 108, Art 5 (c) and (e).

which they are processed.'[532] The limitation factor implied from this principle plays an important role in enhancing the functioning of other personal data protection principles such as minimalism, fair and lawful processing as well as purpose specification principle. Sensitivity is another personal data processing principle. It is to the effect that some types of personal data particularly those concerning someone's political opinions, religious or other beliefs, racial origin, health or sexual life, criminal convictions and other sensitive data should be subjected to more rigorous protection due to their sensitive nature.[533]It is important also to note that the article prohibits automatic processing of sensitive data unless the domestic law provides explicitly for proper safeguards.

Data security is the sixth principle which provides that proper security measures shall be taken to protect personal data stored in computerised data files against unauthorised or accidental destruction, unauthorised access, accidental loss as well as alteration or dissemination.[534]The spirit of this principle is to protect computerised personal data files against intentional or accidental unauthorised destruction, access, loss and alteration, or dissemination. It is worth noting that security measures referred to in this principle must match with the types of data stored, purpose of data in the file and the risk involved while processing the data.[535]

Furthermore, transparency is the seventh principle. This principle has two sides. First, it establishes that any interested person shall be granted the opportunity to determine

[532]Ibid, Art 5 (c) and (d).
[533]Ibid, Art 6.
[534]Ibid, Art 7.
[535]Explanatory report, para 49.

the existence of a computerised personal data file, its main purposes, as well as usual residence or principle place of business of the controller of the file.[536] Secondly, it also states that such a person shall at reasonable intervals and without excessive delay and expense granted an opportunity to obtain confirmation of whether personal data relating to him are stored in the computerised files as well as communication to him of such data in an intelligible form.[537] Rectification is the eighth principle provided in the Convention. It is of the effect that any interested individual shall be allowed to request and afforded the opportunity to verify that data about them are erased or rectified, if such data have been processed in breach of the provisions of domestic laws which uphold the general principles established by Article 5 and 6 of the Convention.[538]Likewise, this principle states that the interested person shall be able to have a remedy when the request for erasure, rectification, communication, or confirmation is not adhered to.[539]

It is important to highlight that the principles as stated in the Convention are not absolute. The Convention also provides for some exceptions to the basic principles. Member states to the Convention are allowed to depart from the basic principles only when the derogation is provided for in the member states domestic law and it constitutes an obligatory measure in a democratic society in protecting state security, public safety and monetary interests of the state or suppression of criminal offence.[540]

[536]Convention 108, Art 8 (a).
[537]Ibid, Art 8 (b).
[538]Ibid, Art 8 (c).
[539]Explanatory Report, para 50.
[540]Convention 108, Art 9 (2) (a).

It is also allowed if it is necessary for protecting the data subject or the rights and freedom of others.[541]

Nevertheless, Bygrave criticises the effectives of the principles of data protection as provided in the Convention 108 on the ground that they are broadly formulated in an abstract way and most of the key words lack definitions. Equally, the Conventions' tendency towards diffusion robs the principles their ability to harmonise domestic laws of the member states. Moreover, feebleness of the Convention is fuelled by the presence of derogation articles in the Convention.[542] As a result, the power or authority of the Convention is undermined and hence fails to stand as applied 'rules of the road' in particular circumstances.[543] Regardless of the criticism, the Convention stands as an international treaty that is legally binding to member states, and hence persuaded the growth and adoption of robust privacy and data protection legislation in and outside Europe.

Together with the general principles, the Convention also provides for the rules of trans-border data flow under the title of chapter three. It is one of the main objects of the Convention to guarantee the flow of personal data among member states. The basic rule is provided under Article 12 which states that a member state shall not restrict the free flow of personal data to the jurisdiction of another member state unless the latter fails to provide equivalent protection for the data.[544]However, the Convention is silent

[541]Ibid, Art 9 (2)(b).
[542]Ibid, Art (3), (6) and (9).
[543]Bygrave, note 528, Supra.
[544]Ibid.

on the situation where personal data flows from a member state to a non-member state.[545]

Nevertheless, the anomaly was remedied by the adoption of an Additional Protocol, which provides for trans-border data flow from a member state to non-member state.[546]Those provisions are nearly identical to the provisions providing for the same in the then Directive 95/46/EC, which was repealed by the General Data Protection Regulation, 2016.[547] It is worth highlighting that the convention applies different standards in dealing with trans-border data flow. The first one is equivalent protection, which is applicable when personal data are transferred from one member state to another.[548]

The second one is adequate level of protection, which is invoked when personal data are transferred from a member state to a non-member state.[549]Arguably, the application of double standard is a weakness of the Convention, which distorts the Councils intention in upholding privacy and data protection rules. Nevertheless, Convention's remains potential as a universal standard. Its open nature, in particular, serves as a base of encouraging the growth of data protection regime at the global arena.[550] It is still relevant in shaping the privacy and data protection regime not only in the CoE but also around the world.

---

[545]Ibid.
[546]Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, ETS No 181.Strasbourg.8XI.2001.
[547]Bygrave, note 543, supra.
[548]Convention 108, Art. 12.
[549]Additional Protocol to the Convention, Art 2.
[550]European Union Agency for Fundamental Rights & the Council of Europe, note 512, supra.

4.3.2 OECD Initiatives

The OECD guidelines on Protection of Privacy and Trans-border Flows of Personal Data (1980) signify international accord on overall guidance regarding the collection and handling of personal data.[551]However, the guidelines are just an annex to the OECD Council of 23rd September 1980, regarding Protection of Privacy and Trans-border Flows of Personal Data.[552]It represents the first international wise towards privacy and personal data regulation.[553]The guidelines were drafted to attain an international coordination of principles as well as providing minimum standards of personal data and privacy protection.[554]The emergence of the OECD guidelines was necessitated by mainly three factors.[555] The first one is the international character of trans-border data flows which called for an intercontinental determination, which only the OECD could provide in that time.[556]

Secondly, it was necessitated by the emergence and spread of technology, which is fast changing with huge capacity to amplify and accelerate the analysis of personal data, with huge capacity of storing information. The development means that personal data and privacy issues as well as other cross-border problems that could not be solved by local laws.[557]The last but not least the changing nature of the law in the last quarter of the 20thcentury from law of nation states with territorial application in states to law

[551]OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publication Service, Paris, France,2001.
[552] Ibid.
[553]Makulilo, note 499, supra.
[554]Olga, E., Y., *Transborder Data Flows and the Sources of Public International Law*. North Carolina Journal of International Law and Commercial Regulation, 1991, Vol 6, Issue 2, pg. 380-416. Accessed from http://www.scholarship.law.unc.edu/ncilj/v16/iss2, on 21st September 2018.
[555]Kirby, M., *The History, Achievements and Future of the 1980 OECD Guidelines on Privacy*, International Privacy Law, 2011, Vol 1, No 1, pp 6-14 at pp 6-8. Accessed from http://academic.oup.com/dp/article-abstract/1/1/6/759637 on 18th Sept 2018.
[556] Ibid.
[557] Ibid.

with international impact and policy necessitated it.[558]Faced with the above challenges the OECD had no option than developing the guidelines to balance the protection of privacy and free flow of information which were published in 23rd September 1980.[559]

The history of the OECD guidelines can be traced back to the creation of the OECD itself. As pointed out earlier (under Section 4.3.1. of this work), it was founded in 1961 to stimulate economic growth as well as world trade. It was created after the recognition of economic interdependence between states. The organisation was thus part of the initiatives to reconstruct the economy that was badly hit by the Second World War. It is of importance to highlight that the OECD is made up of European nations as well as non-European nations.[560]

The unifying factor between member states is economic cooperation. This is clearly supported by Kirby, who postulates that generally the OECD is not dealing with human rights protection but economic cooperation.[561]This contention is supported by Cate and his fellow authors, who contend that one of the original goals of the OECD guidelines is protecting and providing balance between privacy as well as free flow of information.[562]It is in the same vein that Bing posits that the OECD guidelines concentrate on privacy and data protection in line with their impact on economic cooperation and international trade.[563]

---

[558] Ibid.

[559]Cate, F., H., et al, Data Protection Principles for the 21st Century, Books by Maurer Faculty, 2013. Accessed from http://www.repository.law.indiana.edu/facbooks/23, on 18the September 2018.

[560]For a complete list of current OECD member state see note 515, supra.

[561]Kirby, note 558, supra.

[562]Cate, note 559, supra.

[563]Bing, J., *The Council of Europe Convention of the OECD Guidelines on Data Protection*. Michigan Journal of International Law, 1984, Vol 5, Issue 1. Accessed from https://repository.law.umich.edu/mjil/vol5/iss1/13, on 23rd September 2018.

The main thrust of the guidelines lies on the eight privacy and personal data protection principles it provides for. The objectives of the guidelines among other things are clearly summarised in the explanatory memorandum 25 to include attaining acceptance by the state members, principles for minimum standard protection of privacy, and individual liberties with respect to personal data.[564] Additionally, it intends to clear the contradictions and differences between domestic laws and practices that occur within state members to a minimum.[565] Similarly, it aims at making sure that personal data protection accorded in one state furthers the interest of other member states and hence deter the use of undue influence that can be coupled with the flow of personal data to other member states.[566]

Last but not least, it intends to eradicate reasons that may tempt member states to restrict flow of data to other territories due to risks associated with the flow of the same.[567]It is worth noting that the guidelines are technological neutral on the fact that their principles are applicable to both automated as well as manual processing of personal data. The guidelines are also applicable for data in public such national security agencies and the police.[568] Nonetheless, the guidelines are mere recommendation and hence are not legally binding to member states.[569] However, they recommend to member states to take data privacy principles into account when enacting privacy laws in their territories.[570]Correspondingly, they recommend that

[564]Makulilo, note 553, supra.
[565]Ibid.
[566]Ibid.
[567]Ibid.
[568]OECD Guidelines, para 2.
[569]Olga, note 554, supra.
[570]Bygrave, note 547 , supra.

member states should try to eliminate all unjustifiable hindrances to trans-border data flow that can be raised as part and parcel of privacy protection.[571]

The OECD guidelines consist of eight principles of data protection. They include collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguard principle, openness principle, individual participation principle, and accountability principle.[572] In spite of differences in orientation of the OECD and privacy principles, they largely advocate for the same thing.[573]The most notable difference between the two is found in terms of content and not status, especially on the provisions that deal with privacy implementation as well as international cooperation.[574] Those provisions are broader and more elaborate in the CoE Convention than in the OECD guidelines. Similarly, Bygrave posits that data protection principles, as provided in CoE Convention, afford more protection to personal data than provided in the guidelines.[575] This is supported by the fact that the guidelines do not provide for anonymization or destruction of personal data after a lapse of a particular time, as well as the need to have special protection or safeguards for data regarded as sensitive.[576]

Regardless of the weaknesses of the guidelines shown above in some points, they are stronger than the Convention. For instance, the ambits of the guidelines are broader enough to; cover not only electronic but also manual processing of personal

[571]Ibid.
[572]OECD, note 544, supra.
[573]Olga, note 569, supra.
[574]Bygrave, note 571, supra.
[575]Ibid.
[576]Ibid.

data.[577]Additionally, they exemplify openness principle (para 12) in a more boarder way compared to the way it is embodied in Article 8 of the Convention.[578]Moreover, they embody principles for trans-border data between member states.[579]These principles are identical to the equivalent provision provided in the Convention. However, the guidelines go further and highlight their objective of promoting commerce through para 18. They provide that:

> *"Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection".*[580]

It is worth keeping in mind that though the guidelines have some weaknesses and are not legally binding, still they have huge impact in the development of data privacy framework and data protection laws in different nations i.e. Canada, Australia, Japan, Hong Kong, and Australia to mention just a few.[581]They are also the basis of the APEC Privacy Framework.[582]

4.3.3European Union Initiatives

The European Union together with its predecessors (European Economic Community and European Community) lagged behind in regulating privacy when compared to the Council of Europe as well as the OECD.[583] It was not until 1995 when the first instrument known as Directive 95/46/EC was adopted in the EU for regulating

[577]OECD, note 574, supra.
[578]Bygrave, note 576, supra.
[579] OECD Guidelines para 15 to 18.
[580] Ibid.
[581] Bygrave, note 578, supra.
[582] Ibid.
[583] For the definition as well as list of EU member states refer note 495, supra.

privacy. Since its adoption, it established a comprehensive as well as detailed data protection framework and played a crucial role as a changing point for privacy and data protection initiatives in and outside of the EU.[584]It is noteworthy that the EU legal system requires directives to be transposed into domestic laws of its member states to apply.[585] This led to confusion as the directive was transposed differently by different states, and hence varied data privacy rules and regulations across the EU territory.[586]

That is, there were different levels data protection rules, enforcement as well as varied severity of sanctions across the EU.[587] Additionally, there were rapid changes in information technology which affected personal data.[588] The above reasons instigated the need for reform of data protection legislation in the EU.[589] Finally, the reform resulted in repealing Directive 95/46/EC and adopting of the General Data Protection in 2016, which came into force in 25th May 2018.[590]

The General Data Protection Regulation (GDPR) is the EU's binding law which oversees privacy as well as data protection not only for residents but also for citizens of the EU and European Economic area.[591]The GDPR is adopted to harmonise data privacy laws in EU, to eliminate legal fragmentation, intricacies and uncertainties that

[584] Bygrave, note 582, supra.
[585]European Union Agency for Fundamental Rights &the Council of Europe, note 517, supra.
[586]Ibid.
[587]Ibid.
[588]Ibid.
[589]Ibid.
[590]Regulation (EU) 2016/6979 of the European Parliament and of the Council of 27th April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/45/EC (General Data Protection Regulation).
[591]Gilliland, A., T., Issue Brief: The General Data Protection Regulation: What does it Mean for Libraries worldwide? 2018. Accessed from https://library.educause.edu/resources/20185/the-general-data-protection-regulation-what-does-it-mean-for-libraries-worldwide, on 25th Sept 2018.

were caused by the Directive.[592]Likewise, it strengthens privacy rights and data protection laws for all the EU citizens and residents in digital as well as evaluative environment, so that they can be empowered to control their personal data.[593]

Additionally, the new law considers current technological developments, together with implementations on personal data as well as online security.[594] Furthermore, it reshapes the way organisations approach data privacy in the sense that it applies to organisations established in and outside the EU, if they are processing personal data of EU citizen and residence.[595]It is noteworthy that the regulation establishes a single set of rules applicable in all the state members across Europe and hence creates consistency.[596] Additionally, globally the regulation is regarded as the gold standard in the protection of privacy information.[597]

The objectives of the GDPR are clearly stipulated in Article 1 of the regulation which provides that it "lays down rules relating to the protection of natural persons with regard to the processing personal data and rules relating to the free movement of personal data". It is worth noting that the term processing is defined widely to include whatever relates to personal data. This includes activities such as collecting, transferring, storing, using as well as destroying personal data. Moreover, in order to

[592]Chassang, G., *The Impact of EU General Data Protection Regulation on Scientific Research*, Ecancer Medical Science Journal, 2017, 11; 709.Accessed from http://wwwncbi.nlm.gov/pmc/aricles/PMC5243137, on 24th September 2018.
[593] Ibid.
[594]Ibid.
[595]Gilliland, note 591, supra.
[596]Woodrow, H., Privacy Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press. 2018.
[597]Heyink, M. Protection of Personal Information Guidelines for South African Law Firms, 2018. Accessed from http://www.jaa.org.za/doc-manager/protection-personal-information-law-firms-lssa-guidelines-2018, on 24th Sept 2018.

realise its objectives, it comprises seven key principles which one should adhere to when processing personal data. The first one is lawfulness, fairness, and transparency. This principle advocates that personal data should be processed lawfully, fairly, and in transparency manner in relation to the data subject.[598]

Purpose limitation is the second principle with the effect that personal data ought to be collected for specified, explicit as well as legitimate purposes only.[599] Moreover, the latter should be determined at the time personal data is being collected.[600]Data minimisation is the third principle which outlines that personal data collected should be adequate, relevant, and limited to what is required in relation to the processing purposes.[601]Accuracy is another principle which provides that personal data collected and processed should be kept accurate and up to date.[602] This principle entails erasure, removal, or rectification of personal data that are incorrect with regard to the purpose for which they were collected and processed.[603]

Another important principle is storage limitation principle. The principle is to the effect that personal data which are no longer necessary in relation to the purpose for which they were collected or processed must be deleted.[604] However, the principle also allows the retaining of personal data for a longer time if they are processed only for archiving purposes in the public interest, research, and statistical purposes.[605]

[598]General Data Protection Regulation, Article 5(1), (a).
[599] Ibid, Art 5 (1), (b).
[600] Ibid, Recital 39, para 6.
[601] Ibid, Art 5(1), (c).
[602] Ibid, Art 5 (1), (d).
[603] Ibid, recital 39, para 11.
[604] Ibid, Art 5 (1), (e).
[605] Ibid.

Additionally, the regulation provides for integrity and confidentiality principle.[606] This principle advocates for the processing of personal data in a manner that guarantees proper security as well as confidentiality of the data, together with averting unlawful access or use of personal data as well as of equipment used for such processing.[607] The last but not least is the accountability principle. This puts the burden of compliance with the regulation upon the data controller.[608] He or she is not only responsible with compliance but also demonstrating his or her compliance. This can be demonstrated through documenting the manner in which he or she complies with the provisions of the GDPR.[609]

In addition to the data protection principles, the GDPR has a wider scope to the extent of providing for higher standards as well as considerable fines. In the same vein, it provides for remedies, liability, and penalties under Chapter Eight. This entails effective judicial remedies, which include compensation to individuals who suffered material as well as non-material damages.[610] Moreover, the penalties imposed by the regulation are attention grabbing to the management because they are very hefty. For instance, it provides that in case there is a breach of the GDPR, an organisation can be fined up to 4 percent of its annual global turnover or 20million Euros.[611]It intends to make penalties effective, proportionate as well as dissuasive and hence make the management keen on data protection.[612]

[606] Ibid, Art 5 (1), (f).
[607]Ibid, Recital 39, para 12.
[608] Ibid, Art 5(2).
[609] Ibid.
[610] Ibid, Art 77 to 82.
[611] Ibid, Arti 83 (5)
[612] Ibid, Art 83 (1)

Similarly, it provides for trans-border data transfers, except the transfer of personal data to third party countries without an adequate level of protection.[613]It is in the same line that the regulation provides for its extraterritorial application. Arguably, the jurisdiction of the GDPR has been extended to have universal applicability.[614] It is to the effect that it applies to entities processing personal data of EU residents irrespective of companies' location.[615] It is also applicable to the processing of personal data of EU residents by controllers and processors not established in EU if the activities relate to selling of goods or services to Union citizens and the monitoring of conduct, which takes place within the EU member.[616]It is worth noting, that with this extraterritorial jurisdiction, it will continue to be relevant in the United Kingdom despite the outcome of the Brexit.[617]

Furthermore, it reforms or strengthens conditions of consent. The latter is intended to be given through a statement or by a clear affirmative action and must be unambiguous. It is worth highlighting that the regulation provides more rights to data subjects. These include right of access, right to be forgotten, right of notification, right of data portability, right to object the processing of personal data.[618]In addition, the regulation importantly advocates for technological design that will enhance privacy

[613] Ibid, Art 44-50.
[614] Gilliland, note 592, supra.
[615] General Data Protection Regulation, Article 3 (1).
[616] Ibid, Article 3(2)
[617]Vanberg, A., D., & Maunick, M., *Data Protection in the UK Post Brexit: The Only Certainty is Uncertainty*. International Review of Law, Computers & Technology, 2017, 32: 1, 190-206, accessed from http://www.tandfonline.com/action/showCitFormats?doi=10.1080/13600869.2018.1434754, on 20th October 2018.
[618]Ibid, Art 12 to 21.

protection.[619] It also calls for default settings which will enable personal data to be restricted and accessed to a particular number of people.[620]

In addition, the regulation obliges the controllers to enter into contract with vendors or processors who are trustworthy and monitor them for compliance.[621] It also imposes obligation to controllers and processors to designate a data protection officer, if a public authority or body does the processing.[622] Indeed, the GDPR is the most comprehensive privacy law for of age. It is extraordinary in purview and purpose. It is a huge achievement and a key step toward privacy protection. The EU Directive as well as other legislation on data privacy provide a road map and act as a signboard for the robust data privacy regulations in the world. For instance, the POPI Act of South Africa and the Data Protection bill of Tanzania have been developed in line with the EU Directive.

4.4 Asia – Pacific (APEC) Initiatives

The Asia-Pacific Economic Cooperation (APEC) is an economic forum which consists of 21member economies from Asia, Australia, North and South America.[623]It was established in 1989 to develop and strengthen multinational trade relationships, increase the interconnection and affluence of the member economies and encourage

[619]Ibid, Art 25.
[620]Woodrow, note 596, supra.
[621]General Data Protection Article 37.
[622]Ibid, Article 28.
[623]Currently APEC member states are Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Taiwan, Thailand, USA and Vietnam. The members are described as 'economies' because the Cooperation process is mainly concerned with trade and other economic issues and the members regard each other as an economic entity. Accessed from https://www.apec.org/About-Us/About-APEC/Member-Economies, on 20th October 2018.

sustainable, inclusive and innovative economic development in the region.[624]The member economies of the APEC agreed on the need to have a set of mutual principles to guide them on approaching privacy regulations. The agreement is known as the APEC Privacy Framework. It was adopted as a complete version in 2005.[625]This is a set of common principles and implementation guidelines, which, to a large extent, follows the spirit of the OECD. The agreement is known as the APEC Privacy Framework to create operative privacy protections, and hence eliminate barriers to information flows and enhance sustainable trade and economic development in the APEC region.[626]

According to the preamble of the Framework, it intends to promote electronic commerce. It also aims at ensuring free flow of information while at the same time encouraging the development of appropriate information privacy protections within the Asia Pacific region. Additionally, in its wording, the Framework, implicitly does not regard privacy as a fundamental right, but it regards privacy as important for enabling the growth of e-commerce.[627]

The central theme of the Framework is found in the nine Information Privacy Principles (IPPs) it provides. These are preventing harm principles which advocate for the protection of persons against unauthorised collection as well as misuse of their personal data.[628] Secondly, there is notice principle which imposes an obligation on

[624]APEC, (2011) APEC at Glance. Accessed from https://www.publications.apec.org/publication-detail.php?pub_id=1077, on 20th October 2018.
[625]Bygrave, note 584, supra.
[626]Wall, A., GDPR Matchup: The APEC Privacy Framework and Cross Border Privacy Rules,2017. Accessed from https://www.1app.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules, on 21st October 2018.
[627]Bygrave, note 625, supra.
[628]APEC, Privacy Framework, para 14.

the data controller to give notice to an individual whenever the data relating to him are collected and processed.[629] Collection limitation is another principle to the effect that only relevant information, for specified purposes should be collected through lawful and fair means.[630] Further, important to this is the use of personal information principle which entails that personal information should be used to fulfil the intended purpose of collection and other related and compatible purposes.[631] Additionally, choice is another principle, which requires that individuals ought to have choice regarding their personal data with reference to collection, use, disclosure, and transfers.[632]

Moreover, integrity of personal information is another principle, which requires that the information controller should keep records of personal information, which is accurate, complete, and up-to-date as needed with regard to the purposes of use.[633] Similarly, security safeguard is a principle which imposes obligation upon the information controllers to protect personal information against risks such as unauthorised access, destruction, use, modification, disclosure, loss, or any other misuse. Access and correction are also important principles which require that data subjects should have the right to access the data relating to them and to challenge their accuracy and if feasible demand deletion, rectification, completion, or amendment of it.[634]Accountability is the last principle, which imposes obligation to the data

[629]Ibid, para 15, 16 and 17.
[630]Ibid, para 18.
[631] Ibid, para 19.
[632] Ibid, para 20.
[633] Ibid, para 21.
[634] Ibid, para 23, 24 and 25.

controllers to comply with the measures that give effect to the principles of the Framework.[635]

The rules create a protective mechanism for trans-border data transfer within the APEC region as well as providing a pattern for a more wide-ranging global scheme. The above reasons have been a basis of criticising the APEC Framework by different scholars such as Greenleaf[636], Waters,[637] Tan[638] and others. Nonetheless, despite following the spirit of the OECD guidelines, the IPPs as established by the APEC are arguably of lower standard compared to its European counterparts. The main reason for this conclusion is the fact that from the European perspective, privacy protection originates from human right, while from the APEC perspective privacy protection originates from economic relations (for promoting e-commerce and trans-border data flow). This is clearly supported by the fact that the Framework does not include the sensitivity principle like the European instruments. Moreover, the Framework requires adherence to the principle of fair and lawful in the collection stage of personal data but not in processing and further procedures as provided in the European counterparts.[639]Similarly, the Framework does not suggest the way of implementing the principles but left it to the discretion of the member economies.[640]

---

[635] Ibid, para 26.

[636]Greenleaf, G., *The APEC Privacy Initiative: 'OECD Lite' for the Asia- Pacific*, Privacy Laws & Business Journal, 2004, Vol 71, pp 16-18. Accessed from https://www.ssrn.com/so13/papers.cfm?abstract-id-510683, on 24 October 2018.

[637]Waters, N, The APEC, Asia Pacific Initiative- A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation? 2008. Accessed from http://www.austlii.edu.au/au/journal/UNSWLRS/2008/59.html, on 24th October 2018.

[638]Tan, J., G., *A Comparative Study of the APEC Framework-A New Voice in the Data Protection Dialogue?* Asian Journal of Comparative Law, 2008, Vol 3, No 1, pp 1-44.

[639] Ibid, para 18.

[640] Ibid, para 28.

Furthermore, with regard to trans-border data flow the Framework is silent on whether data should be transferred or not to territories without adequate or equivalent privacy protection like the APEC economies. Nonetheless, it imposes liability to controllers who export data to other territories.[641]However, it is important to note in order to cub the gap left by the Framework in cross-border data flow issue and hence realise the goals of the Privacy Framework, the APEC economies adopted and endorsed the APEC Cross Border Privacy Rules (CBPR).[642]

Overall, it is worth noting that nevertheless, the framework initiative is commendable as an important step in achieving a consensus in privacy protection in Asia Pacific region. It is of global importance for representing the readiness of the member economies to devise their own mundus operandi to privacy regulations separate from the ones developed in Europe. It is also inspired Tanzania and south Africa, in Africa, to enact data privacy legislation

4.5 African Initiatives

Like in any other parts of the world, internet penetration and the spread of ICTs have raised concerns on data protection in Africa. However, until recently, African governments were not in the forefront as policy entrepreneurs in privacy and data protection field. Nevertheless, the situation has changed, currently. That is, Africa now is at the forefront and has become the hub of robust and ambitious privacy and data

[641]Bygrave, note 627, supra.

[642]Cousens, A., &Heyder, M., *APEC Privacy Rules for Cross-Border Data Flows-A Model for Global Privacy Protections,* Privacy and Security Law Report, 2015, 14 PVLR 10. Accessed from https://www.huntonak.com/files/uploads/Documents/Center/APEC_Pricacy_Rules_for_Cross-Border_Data_Flows.pdf, on 24th October 2018.

protection initiatives, both at regional and sub-regional levels.[643]It is worth highlighting that currently, 25 countries in Africa have adopted privacy framework legislation or have some established sort of data protection authorities.[644]Apart from the 25 countries, there are also seven countries with data protection bills in place.[645]

Further, the African Union (AU) adopted Convention on Cyber security and Personal Data Protection in 2014[646] to address electronic transaction, personal data protection, and cyber criminality.[647] Developed in line with data protection principles found in the OECD guidelines, the GDPR and other alike international instruments, the Convention provides minimum standards and stands as reference framework for AU member states when formulating data protection legislation.[648]

The scope of the Convention extends generally to private and public sector as well. It also includes computerised and manual processing of personal data.[649]Processing of

[643]Bygrave, L., A., Data Privacy Law- An International Perspective. Oxford University Press, 2014, at pp 80.

[644]O' Donoghue, C., *New Data Protection Laws in Africa.* Data and cyber Security Journal,2015. Accessed from http://www.technologylaw.dispatch.com/20/5/data-cyber-security/new-data-protection-laws-in-Africa, on 25th October 2018.

[645]Currently, countries with Privacy framework include Algeria, Angola, Benin, Burkina Faso, Cape Verde, Comoro, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia, Egypt, Uganda, Nigeria, Western Sahara and Rwanda. Also, important countries with data Privacy bills are Mauritania, Niger, Zambia, Kenya, Tanzania, Malawi and Zimbabwe. Accessed from http://www2.deloite.com/za/en/pages/risk/articles/personal-data-protection-in-africa.html, on 25th October 2018.

[646]Greenleaf, G. & Georges, M., *The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?* 131, Privacy Laws & International Business Journal Report, 2014, pp 18-21, UNSW Law Research Paper No 2015-3. Accessed from https://ssrn.com/abstract=2546652, on 25th October 2018.

[647]Mboizi, J., P., Internet and Data Protection: The African cybersecurity Convention, 2015. Accessed from http://www.linkedin.com/pulse/internet-data-protection-the-african-cyber-security-julius-p-mboizi, on 26th October 2018.

[648]Ibid.

[649]Article 9, African Union Convention on Cyber-Security and Personal Data Protection, 2014. Accessed from https://ccdcoe.org/sites/default/files/document/AU-270614-CSConvention-.pdf, on 22th October 2018.

personal data in relation to research, public security, state security, defence and criminal prosecution are within the scope of the Convention but subject to some exceptions provided by extant law.[650] In addition, the Convention provides for the basic principles of data protection in Article 13 to 23, with which compliance is mandatory by the data controllers. Likewise, it also provides for data subjects' rights in the likeness of the EU approach.[651] These principles include: lawful and fair processing of personal data, processing for specific purpose, legitimacy of processing data based on consent, adequate data collection, collection of relevant data to the purpose only, limited time of data retention, keeping data up to date and accurate as much as possible, and maintaining transparency, security and confidentiality.

Moreover, data subjects' rights include but not limited to access, rectification and blocking, objection of processing and notification. In the same line, the Convention provides for trans-border data flows.[652]It states that data controllers should not transfer personal data outside AU unless the recipient provides adequate level of protection.[653] However, the Convention has not entered into force because it still awaits the ratifications of 15 member states out of 54. In addition, even if the Convention comes into force, before long, it is not going to have any legal force until it is transposed into the domestic legislation of the member states. Likewise, Convention neither provides the definition of the term adequacy, which is one of its principles, nor defines criteria for determining adequacy.

[650]Ibid.
[651]Greenleaf, note 646, supra.
[652]Article 14(6)(a), African union Convention.
[653]Ibid, 14(6)(b).

Additionally, processing of personal data entirely for private use or household activities is not within the ambit of the Convention, except where the data are for regular dissemination or communication to third parties.[654]Moreover, any processing for artistic or literary expression, research or journalistic reasons are exempted. However, this is only if they are conducted solely for literary and artistic expression, research activities or for professional journalism and while adhering to the professional codes of conduct.[655]

Moreover the adequacy criterion does not apply when personal data are transferred to other AU member states regardless of whether they ratified the Convention or not.[656] This might imply that the AU member states who are members of the Convention may assume a provision of their choice. That is when they are required to transfer personal data to other AU member states. Arguably, this may mean that there are no export restrictions or the same adequacy standard as applicable to non-member states.[657] Yet, in some circumstances, it may also be understood to imply that transfer of personal data to other AU member states necessitates approval from the DPA as provided under Article 12 of the Convention. Likewise, the Convention is contrary to the GDPR as well as the CoE Convention 108, which does not advocate free flow of data within member states of the Union and the Convention respectively.[658]

[654] Ibid, Art, 9 (2)(1).
[655] Ibid, Art 14 (3).
[656] Greenleaf, note 651, supra.
[657] Ibid.
[658] Ibid.

Ultimately, these gaps that may slow down the ratification and accession to the Convention. Nevertheless, it furnishes the AU member countries with a framework for personal data protection, which may be transposed to their domestic legislation in near future. Furthermore, it instigates African states to recognise, protect personal data and encourages the free movement of such data.[659] If the Convention is ratified by the member states and enter into force in near future, it will have gigantic impact in developing privacy legislation in African countries. This is due to the fact that the Convention is geared to stand as the reference framework in the quest of developing privacy legislation to the member states.

At sub-regional level, the first initiatives come from the Economic Community of West African States (ECOWAS).[660]This is in the form of a supplementary Act, annexed to the ECOWAS treaty and hence become an integral part of it.[661]The supplementary Act, A/SA.1/01/10 on Personal Data Protection within ECOWAS was adopted in 2010. It legally binds and hence imposes obligation on member countries to enact data protection legislations in their respective jurisdiction.[662] In addition, it is the first binding agreement at regional or international level on data protection in

[659]Deloitte, Privacy is Paramount: Personal Data Protection in Africa, 2017.Accessed from https://www.deloite.com/za/en/pages/risk/articles/personal_data_protection_in_africa.html, on 25th October 2018..

[660]The Economic Community of West African States was established in 1975. It is a 15-member regional group with the mandate of promoting economic integration in all fields of activity of the constituting countries. Its members states include Benin, Burkina Faso, Cape Verde, Cote d' Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal and Togo. Accessed from http://www.ecowas.int/about-ecowas/basic-information/, on 25 October 2018.

[661] Bygrave, note 643, supra.

[662]Orji, U., J., *Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act*. International Data Privacy Law, 2017, Vol 1, Issue 3, pp 179-189. Accessed from http://www.academis.oup.com/idpl/article-abstract/7/3/179/4211051?redirectedFrom=fulltext, on 26the October 2018.

Africa. The agreement is developed following the spirit of the repealed EU Data Protection Directive.[663] Besides, two third of the ECOWAS member states have enacted data protection laws[664] and bills for the same are in the process in Niger. Hitherto, six ECOWAS states have not taken notable initiatives in developing data protection regulations at domestic level.[665]

In addition, the Southern African Development Community (SADC)[666] has developed a Model Law on Data Protection (here in referred as the law) in 2012 for the southern African countries.[667] The law is made in line with the then European Directive 95/46/EC, which is now repealed and replaced by the GDPR, 2016. Correspondingly, its contents are developed largely, in line with the AU Convention on Cyber Security and Personal Data Protection, as well as the supplementary Act, A/SA.1/01/10 on Personal Data Protection within ECOWAS. The law was intended to establish uniformity in the protection of individual rights and freedoms with reference to the processing of personal data throughout SADC region. As its preamble shows, the law intends to protect the rights and freedoms of individuals and promote trans-border data flows within SADC Region. With this rationale in mind, Article 2 of this law was

[663]Greenleaf, G., & Georges M., African Regional Privacy Instruments: Their Effects on harmonization, Privacy Laws and Business International Report 19-21, UNSW Law Research Paper No. 2015-10, December 2014. Accessed from https://www.ssrn.com/abstract=2566724.

[664] These include Benin, Burkinafaso, Cape Verde, Senegal,Ghana, Ivory Coast, Nigeria, and Mali. Ibid.

[665] These include Togo, the Gambia, Guinea Bissau, Liberia and Sierra Leone. Ibid.

[666]Currently, SADC member states are Angola, Botswana, Comoros, Democratic Republic of Congo, Swaziland, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia and Zimbabwe. Accessed from https://www.sadc.int/member-states, on 26th October 2018.

[667]Wanyama, E., What African Countries can Learn from European Privacy Laws and Policies, 2017. Accessed from https://www.cipesa.org/2017/07/what-africa-can-learn-from-european-privacy-laws-and-policies, on 26th October 2018.

adopted to settle which rules applies when and to whom and to harmonise the application of rules and regulation in relation to data protection across SADC region. Besides, similar to the EU Directive, AU Convention and the Supplementary Act of the ECOWAS, the law is not applicable to any processing of personal data by an individual in the course of doing personal or household activities.[668]

Structurally, this law is made up of a preamble and fourteen chapters, but without recitals like other privacy legislations such as the EU Directive. Although the law does not precisely define its objectives, these can be generally inferred from the wording of the preamble. The scope of the Model-Law set in chapter 2 that the law applies to automated, partly automated as well as manual processing of personal data.[669] Similarly, it applies to public as well as private data controllers.[670]In addition, the scope of the Model-Law encompasses territorial applicability. The law has a wide scope as the then EU Directive.[671] This is evident under Article 2 (2) of the law, which provides that his Model-Law is applicable: -

(a) to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established on [given country] territory or in a place where [given country] law applies by virtue of international public law;

(b) to the processing of personal data by a controller who is not permanently established on [given country] territory, if the means used, which can be automatic or other means is located in [given country] territory, and is not

[668] SADC Model-Law 2012, Art 2(4).
[669]SADC Model-Law 2012, Art 2 (1).
[670]Ibid, Art 1(3).
[671] EU Directive /95/46/EC, Art 4.

> the same as the means used for processing personal data only for the purposes of transit through [given country] territory.

It worth noting that Article 2, cited above comprises two different sets of rules of laws applicable. First, are the rules applicable to SADC member states and secondly, are those relating non-SADC member states.

Furthermore, the law contains seven basic principles or conditions accepted for the processing of personal data. The principles adopted in the law are similar to those established in EU Directive, AU Cyber Security Convention, the supplementary Act as well as other international instruments on privacy and data protection. The principles include fair and lawful processing,[672] purpose specification,[673] legitimacy,[674] sensitivity,[675] accountability,[676] security[677] and data quality.[678] Apart from the data processing principles, the law also establishes the data protection authority. It is empowered to supervise and control the Model-Law as well as the privacy rights in the national territory.[679]

Likewise, the law imposes some obligations to the data controllers. The law obliges the data controller to provide information to the data subject before processing data about him/her.[680] Moreover, the data controller is required to take reasonable technical

[672]Ibid, art 12.
[673]Ibid, art 13.
[674]Ibid, art 14.
[675]Ibid, art 15.
[676] Ibid, art 30.
[677]Ibid, art 24.
[678]Ibid, art 11.
[679]Ibid, art 3.
[680]Ibid, art 21.

and organisational measures to safeguard security of the data.[681] Other obligations include accountability,[682] confidentiality, to maintain openness of processing[683] and notifying the data protection about the processing of personal data.[684]

In addition, the SADC Model-Law provides for the rights of the data subject in part seven.[685] Like the obligations of the data controllers, the rights of the data subjects are in line with the EU Directive, the AU Convention on Cybersecurity as well as the ECOWAS Supplementary Act. These include the right of access, rectification, deletion, temporary limitation of access, right of objection and the right of representation if the data subject is a minor. Moreover, the Model-Law encompasses the rules of trans-border data flow. However, the rules provided differ from what other instruments such as EU Directive and the AU Cyber Convention and others on the fact that it prohibits transfer of personal data not only the third-party countries without adequacy level of protection but also to SADC members who have not adopted the Model-Law. Arguably, the provision above defeats the object of the law, which is harmonization. Yet, the provision has some merits that it may compel or motivate SADC member states to develop and adopt privacy regulations that that in the same line with the Model-Law.

Therefore, regardless of the fact that though SADC Model-Law is a soft law, upon ratification it is likely to influence the development and enactment of data privacy laws in Tanzania and South Africa respectively. This is mainly aggravated by its

[681]Ibid, art 24.
[682]Ibid, art 30.
[683]Ibid, art 29.
[684]Ibid, art 26.
[685]Ibid, art 31-37.

requirement of prohibiting transfer of personal data to SADC member states, which has not adopted data privacy laws in line with the Model-Law. Moreover, due to the fact that the Model-Law was made in line with EU Directive, which is now repealed, there is a dire need of the SADC to revisit the law so that it can be amended and bridge the gap that is bridged by the GDPR to its predecessor the Directive.

In the same line, the East African Community (EAC)[686] like other regional blocs had its own initiatives to ensure protection of personal data and privacy in its region. However, unlike its counterparts of ECOWAS and SADC the EAC did not adopt legislation for data protection and privacy but issued a legal Framework for Cyber Law in 2008. The framework was adopted in 2010, with the intention of calling its member states to adopt legislation protecting personal data in line with international standards and the best international practice.[687]

The main thrust of the EAC Legal framework for Cyber Law is to harmonise the policies and regulation in the East African Community. Indeed, the framework is developed in response to the challenges brought by the development of ICTs and the increasing reliance to it in doing day to day activities be it commercial or administrative, especially the use of internet.[688]Further, as pointed out above, the EAC framework differs from other Frameworks, especially in privacy and data protection field. It is argued by *travauxpreparatoires* that the Framework is not a model law but

[686]East African community member states include Burundi, Kenya, Rwanda, South, Sudan, Tanzania and Uganda. Accessed form https://www.eac.int, on 26th October 2018.

[687] Bygrave, note 661, supra.

[688]Walden, I., East African Community Task Force on cyber Law: Comparative Review and Draft Legal Framework, Draft v.1.0.2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008, p.8. Cited in Makulilo, note 423, supra.

rather A sheer recommendation to the EAC member states to refer to them when developing domestic cyber laws, and hence not intended to be binding.[689]

Similarly, in the data privacy field the *travauxpreparatoires r*ecommended the imposition of two obligations that regulate processing of persona data. First, it recommends that in processing personal data, member states should ensure compliance with some principles relating to good practice. The term good practice, as used here, entails accountability, transparency, fair and lawful processing of data, data security, data accuracy and processing limitation.[690]Second, it recommends to member states to furnish the data subject with a copy of their personal data collected and processed, as well as an opportunity to correct any incorrect data held about them.[691]

Likewise, the Cyber Framework encompasses a recommendation that due to the significance of privacy and data protection, among other things, member states should fully take into account the existing international best practices in processing personal data.[692] However, the Framework did not go further to mention any of such best practices. In addition, the Framework did not attach any annex of such best practice or any international code of data privacy as it is generally done to other Frameworks. Arguably, the omission may defeat the object of the Framework, that is the harmonization of data privacy regulation in the region. This is because it may lead the

[689]Ibid, p 9.
[690]Ibid, p 17.
[691]Ibid.
[692]EAC, EAC Legal Framework for Cyber Laws, (Phase I), pp 17-18.

member states to adopt and follow some international best practices of their choice and hence differ with the other.

It suffices to say that though EAC adopted the Cyber Framework Phase I in 2008 and Phase II in 2011, which addressed several issues data protection inclusive, the Framework has yielded some minor tangible results in data privacy protection in EAC eight years since the adoption. That is, only the country of Uganda in the EAC has developed data protection legislation since then. Other visible efforts are the data protection bills in place in some countries. The main reasons include non-binding nature of the Framework, lack of clearly stipulated minimum standards of data protection principles for the member states to stick to. Tanzania being one of the member states in EAC has not progressed towards the enactment of data privacy regulation. There is only a draft bill of the same that has been pending since 2014.

Regardless of the common and divergent approaches to privacy, the regional, sub-regional and national initiatives for privacy embody almost some common privacy principles. The principles originate from European instruments. These include choice and consent, notice, data quality and integrity, data security, data retention and destruction, data access and correction, cross border data transfer, personal data breach notification, registration with the DPA, and lastly appointment of the Data Protection Officer (DPO). However, not all the instruments provide for all the principles mentioned above.

To sum this section, it is worth noting that cross-border trade and advancement of technological innovation have transformed Africa in many ways and made the claim

of privacy imperative. The African initiatives for privacy protection are evidence that this is an evolving concept. It affirms that privacy concept, to a large extent, acquires the status of a human right in Africa. However, regardless of all the efforts, there is a problem of harmonisation of privacy laws in Africa. This is due to the fact that there are disparities in policies and regulations adopted for privacy protection at the regional, the sub-regional and at the national level.

4.6 Conclusion

Cloud computing technology is a recent development, which postdates all the international instruments discussed in this part. As a result, the available international instruments suffer limitation of addressing privacy and security issues in the cloud. That explains why within EU new initiatives of repealing old laws and coming of new laws such as the GDPR. In the same line, COE has been revised and OECD Guidelines has been revised as well. The main reason is that these instruments had a very huge limitation in drafting and hence the instruments were not technological neutral. Moreover, the AU Convention though enacted in 2014 lacks a lot compared to other international instruments in content. Further, the instrument has not even come into force so it limits in highlighting the privacy and security challenges in the Cloud.

Similarly, review of the international benchmarks for privacy portrays some shared and disparate trends. Firstly, the majority of the international human rights instruments provides for the privacy right. Nonetheless, that right is framed very widely to the extent that it fails to provide proper protection of privacy and personal data. Yet, it has provided a firm foundation for the emergence and growth of privacy laws in the world. Secondly, there are different approaches for protection of data privacy. For instance,

the European approach originates from human right and a comprehensive approach is more favoured, coupled with a data protection framework and unified supervisory authorities. Yet, in other areas like the APEC region, the approach is more business oriented, while the industry self-regulation is more preferred in the USA. Similarly, in Africa, privacy is still in nascent stage, and the favoured approach is mainly the European model, as privacy concept is imported from Europe.

Thirdly, the presence of international, regional, and sub-regional commitments accepted by different nations raises some multi-sectoral effect of the privacy policies and frameworks. They compel those relying on industry self-regulation to be influenced by the principles applied in comprehensive approach mode. Fourthly, regardless of having international instruments on privacy and data protection, the GDPR and its predecessor, the Directive 95/46/EC of the EU prove to be the most significant catalyst for the growth of privacy and data protection regulation in the world. This is mainly due to its extraterritorial application through the adequacy requirement before transferring personal data to non-member states. Thus, countries wishing to engage in transaction involving personal data transfer are indirectly compelled to adopt comprehensive privacy regulation to meet the European standards. Indeed, the GDPR and its predecessor have a global impact and can be rightly regarded as the main catalyst for growth of robust privacy and data protection regime.

CHAPTER FIVE

PRIVACY AND SECURITY REGULATION IN THE CLOUD IN TANZANIA

5.1 Introduction

The need to provide legal protection for security and privacy of personal data in international regulation cannot be overstressed. In the same line, Tanzania is a signatory of international human right treaties such as the ICCPR, 1966; the United Nations Declaration of Human Rights, 1948 and a member of SADC with its Model Law of Data Protection, 2012, which is relevant to privacy and data protection. This implies that Tanzania is bound to implement the international Human rights treaties above as well as the SADC Model Law of Data Protection at domestic legislation.

In this chapter, the researcher analyses the system of security and privacy regulation and protection available in Tanzania. It is worth noting that the thesis mostly uses the term privacy instead of privacy in the cloud because there is no clear demarcation between the terms. The decision has also been informed by the fact that the term privacy in the cloud is rather new in the privacy discourse in Tanzania. Similarly, whereas, intellectuals and non-intellectuals struggle to understand what is meant by privacy in the cloud, the term privacy is more comprehensive to both intellectuals as well as non-intellectuals. Secondly, despite being significant for global audience, the thesis specifically focuses legal reform agenda in Tanzania. With this idea in mind, it is not proper to employ a term that is unfamiliar to many Tanzanians. Thirdly, privacy in the cloud is a subset of privacy right in general. This implies that protection of privacy in general is a prerequisite for protection of privacy in the cloud. The latter cannot exist without the former.

5.2 Privacy and Security Regulation

Tanzania has had complicated and difficult journey in protecting privacy right of its residents and citizens. This includes deterring the inclusion of bill of rights in its constitution soon after independence to futile attempt of enacting data privacy legislation in the draft of freedom of information bill in 2006.[693] This implies that privacy regulation in Tanzania is undeveloped, regardless of the fact that the ICT has deluged Tanzania as most people use ICT in everyday life. Currently, Tanzania has no comprehensive privacy protection regulation. That, it only has a draft Data Protection Bill, but which has been pending since 2014.[694]In the absence of legislation, it protects privacy of its citizens through the constitution, statutory legislation, and somewhat through common law.[695]

The main source of privacy right in Tanzania is its 1977 Constitution as amended from time to time. Other sources are several statutory provisions in various pieces of legislation which when the need arises provides for privacy issues.[696]Case law is regarded as the third source. Nevertheless, it is undeveloped and hence of slight significance at present.[697]This part appraises the above-named sources and how they provide the basis of privacy protection in Tanzania at present. Nonetheless, more emphasis is placed on communication, health, and national security sectoral laws. This is because these sectoral laws, largely extent, in an ad-hoc style, provide for privacy

[693]Boshe, P., Data Privacy Law Reforms in Tanzania in Makulilo, A., B., (ed) African Data Privacy Laws, Switzerland, Springer, International Publishing AG,2016, Pp 161-187.
[694] Ibid.
[695]Makulilo, note 564, supra.
[696] Ibid.
[697] Ibid.

issues.

5.2.1 Privacy, the Constitutional Right

Privacy is a right recognised and guaranteed by the Constitution of the United Republic of Tanzania in Article 16. It provides inter alia that, "every person is entitled to respect and protection of his person, the privacy of his own person, his family, and of his matrimonial life, and respect and protection of his residence and private communications"[698]Nevertheless, privacy right as provided in the Constitution is not absolute. Like any other fundamental rights, it is limited by other articles from the same Constitution.

Article 16 (2) provides specific restrictions of that right when it states that "for the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner, and the extent to which the right to privacy, security of his person, his property, and residence may be encroached upon without prejudice to the provisions of this Article. This implies that the implementation of privacy right may depend upon other legislation to give effect and state its enforcement mechanisms.[699] Furthermore, its enforcement is embedded to the other fundamental rights and can be contravened in favour of public safety and national security.[700]It is worth of note that the Constitution gives a room to other laws to encroach privacy right.

[698]The Constitution of the United Republic of Tanzania, 1977. Article 16 (1).
[699]Boshe, note 694, supra.
[700] Ibid.

In addition to the specific limitation to the privacy right as provided in article 16 (2), there are also general restrictions which are applicable to the bill of rights as enshrined in the Constitution. These are conditions provided under Article 30(2) through which any provision in the bill of rights may be limited. The Article provides that:

> *"It is hereby declared that the provisions contained in this Part of this Constitution which set out the principles of rights, freedom and duties, does not render unlawful any existing law or prohibit the enactment of any law or the doing of any lawful act in accordance with such law for the purposes of: - (a)ensuring that the rights and freedoms of other people or of the interests of the public are not prejudiced by the wrongful exercise of the freedoms and rights of individuals; (b) ensuring the defence, public safety, public peace, public morality, public health, rural and urban development planning, the exploitation and utilization of minerals or the increase and development of property of any other interests for the purposes of enhancing the public benefit; (c) ensuring the execution of a judgement or order of a court given or made in civil or criminal matter; (d)protecting the reputation, rights and freedoms of others or the privacy of persons involved in any court proceedings, prohibiting the disclosure of confidential information or safeguarding the dignity, authority and independence of the courts; (e)imposing restrictions, supervising and controlling the information, management and activities of private societies and organizations in the country; or (f) enabling any other thing to be done which promotes or preserves the national interest in general."*

In the spirit of Article 30 (2), the Court of Appeal of Tanzania has established through case law, the legal standards which must be met when any other law seeking to restrict or contravene the fundamental rights of an individual. In *Christopher Mtikila versus The Attorney General*, the court held that "a law which seeks to limit or derogate from the basic right of the individual on grounds of public interest will be declared unconstitutional unless it satisfies two requirements: that it is not arbitrary and that the limitation imposed by laws is no more than is reasonably necessary to achieve the legitimate objection."[701] These requirements entail that the law should be accepted to

[701]*Christopher Mtikila v Attorney General,* Miscellaneous Cause No.10 of 2005, High Court of Tanzania, Dar es Salaam (Unreported). Accessed from http://www.elaw.locusattorneys.co.tz/ content/christopher-mtikila-versus-attorney-general, on 10th November 2018. See also,*Kukutia Ole*

be lawful. This implies that the law should establish proper safeguards and control against arbitrary decisions as well as abuse of the law by the authority when applying the law.

Moreover, the limitation imposed to the basic right should be proportional to what is required to achieve the legitimate results. The High Court of Tanzania has adopted the same position in *Jackson Ole Nemeteni and 19 Others versus the Attorney General*, when it established that in the need of a procedure set by law, the application of a provision of any law that intends to limit the fundamental rights of an individual is prone to abuse, and hence cannot fall within the ambit of Article 30(2) of the Constitution.[702]Regardless of the constitutional limitations to the right of privacy, it establishes a normative basis for privacy regulation in Tanzania.

5.2.2 Draft Data Protection Bill

Despite the fact that there is no comprehensive data protection legislation in Tanzania to date, there is a draft Data Protection Bill, which is pending since 2014. With the help from the Support to the Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA) the Ministry of Communication drew the Draft Bill.[703] Further, the Draft Bill was communicated to a limited number of stakeholders only not the general public.[704] Likewise, Tanzanian Law Reform Commission initiated a consultation with the public in 2016 so as to collect public opinions to inform the proposal on data

Pumbuni and Another v Attorney General and Another (1993) TLR 159 at p.167, See also, *Director of Public Prosecutions v Daudi Pete* [1993] TLR 22; *Julius Ishengoma Francis Ndyanabo v Attorney General* (2004) TLR 14.

[702]Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam (Unreported).

[703]Boshe, note 700, Supra.

[704] Ibid.

protection legislation.[705] However, to date, the status of that initiative remains unknown to general public. The Draft Bill though is yet to be passed as a law; is discussed at this part because changes recommended may possibly be made to the final text of the legislation.

The Draft Bill proposes a wide-ranging framework for data protection, which intends to regulate processing of personal data by private and public sectors irrespective of whether the processing is through automated means or not. The bill is applicable to personal data regardless of the format or media used: it can be in electronic means, printed document, filmed, taped, or otherwise.[706] It does not encompass, any processing of personal data for by or on behalf of the state, which may include processing for public safety, defence, or national security, or for the purpose of preventing, investigating, or proof of offences.[707]This necessarily implies that principles and other provisions of the bill are not applicable to the in law enforcement and criminal law filed of law.

The draft Data Protection Bill establishes the Data Protection Authority (the Data Protection Commissioner) responsible with the implementation of the bill.[708]Correspondingly, the draft bill provides for the data protection principles, also known as the conditions for the lawful processing of personal data. These include lawful purposes for collection of personal data, with transparency and lawful means

[705]Makulilo. A., B., and Boshe, P. Consultation on the Commission's Comprehensive approach on Personal Data Protection in Tanzania, 2016, submitted on 31st August 2016.
[706]Boshe, note 703, supra.
[707] Draft Data Protection Bill, S, 5, (3), (b).
[708] Ibid, s.20.

of collection.[709] Equally, use limitation is another principle with the effect that data should be used for the intended purpose of collection only.[710] Similarly, there is purpose specification,[711] data retention, data security,[712] data accuracy,[713] accountability[714] and data subject participation.[715]

Although the draft bill provides for the data protection principles as well as establishing the office of the Data Protection Commissioner, it does not stipulate other necessary conditions to be adhered to before processing personal data. For instance, the condition of giving notice to the data protection Commissioner is not explicitly stipulated. The bill is also silent with regard to consent requirement while it is a prerequisite condition to be met for the processing of personal data to be lawful. Arguably, if the draft bill is passed into law without any substantial change, it will offer only minimum data processing conditions and principles. Nevertheless, with the current operation of the European Union General Data Protection Regulation, (GDPR) with its universal applicability, the draft bill might not attain the adequacy requirement of the EU law. The GDPR restricts transfer of European personal data to third countries (non-EU member states) unless they attain the adequate standard of data protection in relation to the GDPR.

[709] Ibid, s, 6, (1).
[710] Ibid, s, 9.
[711] Ibid, s, 10.
[712] Ibid, s, 12.
[713] Ibid, s. 8.
[714] Ibid, s.15.
[715] Ibid, s. 7 and 14.

5.2.3 Privacy and Security Protection in Communication Sector

Despite the general understanding that a comprehensive privacy regulation is missing in Tanzania, to some extent, privacy is protected through some sector specific regulations.[716] Communications sector is among the sectors with laws and regulations with some provisions for protecting privacy. One of those is the Electronic and Postal Communication Act, 2010, (EPOCA). This Act was enacted not only with the aim of addressing the challenges that came with modern technologies, but also harmonising and consolidating communication related laws so as to enhance their implementation.[717] More so, it was also intended to introduce the registration of sim cards as well as Central Equipment Identification Register (CEIR).[718]The law requires every person who owns or intends to own and use a mobile telephone in the country to register his or her sim card.[719]

Similarly, it requires all the service providers to collect for registration purpose information which identify all the buyers of sim cards before activating the same in their networks.[720] Likewise, the Act stipulates specific information that a potential customer should submit to the service provider. A natural person ought to give his or her full name, proved by a copy of the identity card or any other accepted documents in proving the identity of an individual, together with residential, business, or registered physical address.[721] Correspondingly, a legal person is required to submit any of the following: certificate of registration, business license, Tax Payer

[716]Makulilo, note 695, supra.
[717]Electronic and Postal Communications Bill, 2009, 'Objects and Reasons' at p.115.
[718]Ibid.
[719] EPOCA, 2010, section 93(1.)
[720] Ibid, section 93(2).
[721] Ibid, section 93(2)(a).

Identification Number Certificate, or a Value Added Tax Registration Number if applicable.[722]

The service provider is duty bound to verify the accuracy of collected information before registering the subscriber.[723] The Act stipulates that the register should be retained either in hard copies or electronically.[724]Additionally, the law requires that the personal information collected by the services provided be submitted to the Tanzania Communications Regulatory Authority (TCRA) for safekeeping in the subscribers' database.[725]

EPOCA places a duty of privacy protection upon the service providers owing the fact that the data subject loses control over his her data once collected and stored in the database.[726]It provides that "a person, who is a member, employee of application service license, or its agent, shall have a duty of confidentiality of any information received in accordance with the provisions of this Act."[727] Furthermore, it states, "no person shall disclose the content of the information of any customer received in accordance with the provisions of this Act, except where such person is authorized by other written law."[728]Arguably, this duty intends to make sure that personal information collected are secure, confidential and intact.

[722] Ibid, section 93 (3)(b).
[723] Ibid, section 93(3)(b).
[724] Ibid, section 93 (4).
[725] Ibid, section 91 (1), (2), (3).
[726] Ibid, section 98.
[727] Ibid, section 98 (1).
[728]Ibid, section 98 (2).

As shown above, the provision applies only to members, employees and agents,as the TCRA remains to be the custodian of the personal information collected, according to section 91. Nonetheless, EPOCA is silent on the TCRA's duty on privacy protection. Similarly, although Section 99 may be impliedly applicable to the TCRA, it does not sufficiently bring it within its domain.[729]Moreover, Section 98 (2) of EPOCA authorises disclosure of information, if the individual disclosing the information is authorised by any other written law. However, the phrase "any other written law" is very wide to the extent of jeopardising privacy of personal data collected under this law. Additionally, EPOCA permits interception through Article 99, which allows interception as well as disclosure if the information is needed for use by the court of law, law enforcement agency, or a tribunal.[730]The section also allows disclosure of information by an authorised person to another law enforcement officer so as to enable them to perform their official duties properly.[731]

Similarly, EPOCA criminalises unlawful interception, disclosure, or use of information obtained unlawfully.[732] More so, the criminality character is also

[729] Section 99 of EPOCA states, A person shall not disclose any information received or obtained in exercising his powers or performing his duties in terms of this Act except (a) where the information is required by ant law enforcement agency, court of law and other lawfully constituted tribunal; (b) Notwithstanding the provision of this section, any authorized person who executes a directive or assist with execution thereof and obtains knowledge of information of any communication may- (i) disclose such information to another law officer to the extent that such disclosure is necessary for the proper performance of the official duties of the authorized person making or the law enforcement officer receiving the disclosure; or (ii) use such information to the extent that such use is necessary for the proper performance of official duties.

[730] Ibid.

[731] Ibid.

[732] Section 120, EPOCA states; Any person who, without lawful authority under this Act or any other written law (a) intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or (b) Discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through interception of any communications in contravention of this section; or (c) Uses, or attempts to use the contents of any communications, knowingly having reason to believe that the information was obtained through the interception of any communications in contravention of this

applicable when an authorised person lawfully intercepts the contents of communication and eventually discloses them unlawfully.[733] However, the possibility of enforcing these provisions is very minimal considering that the provisions are drafted very broadly and loosely. Arguably, assessing these provisions while referring to the constitutional right of privacy as provided in the Constitution, clearly implies that EPOCA does not properly protect personal data held in the service providers' database and those in the TCRA's database. Similarly, the flimsy protection of data privacy accorded by EPOCA does not apply to the cloud. Though the Act stipulates that data may be stored electronically, it does not categorically provide for the cloud environment.

In the same line, the Electronic and Postal Communications (Consumer Protection) Regulations contain some conditions and principles for processing personal data in communication sector.[734]The Regulations are applicable only to those entities registered to offer postal services and electronic communication services.[735]The regulation permits the licensee to collect and maintain personal data of his or her customers where necessary for business purposes only.[736] In so doing, the collection

section, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both.

[733] Section 121, EPOCA states; (1) Any person who is authorized under this Act intentionally discloses, attempts to disclose, to any other person the contents of any communications, intercepted by means authorized by this Act; (a) knowing or having reason to believe that the information was obtained through the interception of such communications in the connection with a criminal investigation, (b) having obtained or received the information in connection with a criminal investigation; or (c) improperly obstructs, impedes, or interferes with a duly authorized criminal investigation, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both.

[734]Electronic and Postal Communications (Consumer Protection) Regulations, 2018, R.6, Accessed from https://www.tcra.go.tz/images/documents/regulations/10._GN._61__The_Electronic_and_Postal_Communicat ios_Consumer_Protection__Regulations_2018.pdf, on 21 November 2018.

[735] Ibid, Regulation 2.

[736] Ibid, Regulation 6 (1).

and maintenance must comply with the general data processing principles. These include the principle that personal data should be fairly and lawfully collected and processed.[737]

Secondly, any processing of personal data must be for the identified purposes only.[738] Thirdly, the processing of data should be accurate and should be based on accurate information.[739] Fourthly, any processing of personal data should be done in agreement with other consumer's rights.[740] Fifthly, the personal information collected should be protected against improper or accidental disclosure.[741] Lastly, personal data should not be transferred to any party except as permitted by the terms and conditions agreed with the consumer, as permitted by any permission or approval of the TCRA, or is otherwise permitted or required by other applicable laws.[742]

It is worth noting that the regulation provides a basis of personal data protection in communication sector. However, the protection of personal information in other divisions is not within the ambit of the regulation. Similarly, the regulation does not provide for consent, which is a very important prerequisite for the processing of personal data. More so, the regulation does not provide for period within which personal data can be retained in the database of the service provider be it public or private entity. The lack of retention period provision poses a risk of personal data being retained for an indefinite time. Likewise, the regulation is silent on the rights

[737] Ibid, Regulation 6 (2), (a).
[738] Ibid, Regulation 6 (2), (b).
[739] Ibid, Regulation 6 (2), (c).
[740] Ibid, Regulation 6 (2), (d).
[741]Ibid, Regulation 6 (2), (e).
[742] Ibid, Regulation 6 (2), (f).

accorded to the data subjects. These include rights such as right of rectification, right to access personal data, right of erasure, and the right to be informed about the data that different entities have about them.

Similarly, the Electronic and Postal Communications (Online Content) Regulations establish some regulations which help in boosting privacy and data protection in communication sector.[743]The regulations are applicable only to the online content. They regulate the online services offered by the application services licensees, bloggers, internet cafes, online content hosts, online forums, online radio, or television, social media, subscribers, users of online content, and any other related online contents.[744]Moreover, the regulations vest powers upon the TCRA to regulate the online content.[745] This is accomplished through registering users as well as platforms of online content and through actions such as ordering the removal of prohibited content or removal of contents that violate specified obligations and running a public awareness in relation to proper and safe use of online content.[746]It is in the same line that Part 3 of the Act provides for specific obligations of the service providers and the users of online services and platforms, including the discussion forums, social media and online broadcasts, which include radios and television.

[743]The Electronic and Postal Communications (Online Content) Regulations Act, 2018. Accessed from https://www.tcra.go.tz/images/documents/regulations/SUPP_GN_NO_133_16_03_2018_EPOCA_ONLINE_CONTENT_REGULATIONS_2018.pdf, on 12th December 2018.
[744] Ibid, Regulation 2 (a)-(i).
[745] Ibid, Regulation 4.
[746]Ibid, Regulation 4 (a), (b) and (c).

Additionally, the regulation enhances privacy and data protection initiatives in the country through, prohibiting unlawful disclosure of any information collected or obtained by the TCRA and any of its employees while performing their lawfully duty or while exercising their powers.[747]However, this prohibition is subject to exception when any law enforcement agency, court of law, or any other lawful constituted tribunal necessarily needs the information.[748]Nevertheless, the regulation restricts the processing of the information only to the extent that is required for the proper performance of the lawful duties.[749]

Despite the fact that the Act promotes privacy and data protection initiatives, its applicability to the online content only, is a grave limitation. This is because it cannot be applied to offline data irrespective of their sensitivity. Moreover, the applicability of the Act to all online data content is very broad in the sense that not all online data qualifies as personal data. Furthermore, the Act is silent on the retention time of an online content. This implies that data, personal data inclusive, may be retained for unlimited time contrary to data protection principles. Arguably, the Act does not provide for data subject rights whenever personal data is processed by the TCRA or in the online content. These include rights such as right to rectification, access, right to be forgotten, and many others.

[747] Ibid, Regulation 11 (1).
[748] Ibid.
[749] Ibid, Regulation 11 (2).

5.2.4 Health Sector

The growth of electronic health records under the umbrella of health information technology is being promoted all over the world.[750] The Tanzania National Health Strategy 2013-2018, among other strategic principles provides that e-Health should uphold integrity, patient data privacy and confidentiality.[751]Regardless of the fact that there are neither specific e-health regulations nor comprehensive data privacy legislation in the country, there is some legislation in the health sector with some provisions relating to privacy protection in the health sector.

HIV and AIDS (Prevention and Control) Act, 2008 is one of the legislations in the health sector that provides for privacy protection. The Act criminalises some actions and practices of health workers. Subjecting a person to the testing of HIV without his or her consent or knowledge is among the practices criminalised by the Act.[752]In establishing criminal liability under this Act, consent and knowledge are two separate elements but inseparable ones. This is due to the fact that there is no consent without knowledge, and knowledge alone without agreement does not justify HIV testing. Ultimately, any testing with knowledge but without agreement amounts to testing without informed consent and hence a crime on the part of health practitioner.

---

[750]Verhenneman, G., &Dumortier, J., *Legal Regulation of Health Records: A Comparative Analysis of Europe and the US* in George, C., Et al, eHealth: Legal, Ethical and Governance Challenges. Springer, Heidelberg/New York/Dordrecht/ London,2013, Pp 25-56, at p.25.

[751]Tanzania- Ministry of Health and social Welfare Tanzania National eHealth Strategy 2013-2018, 2013, p 7 Accessed from http://ihi.eprint.org/3727/1/ehealth_strategy%20august%2029th/20sept%202013, on 25th November 2018.

[752]Section 15(7) of the HIV and AIDS (Prevention and Control) Act which states, 'Any health practitioner who compels any person to undergo HIV testing or procures HIV testing to another person without the knowledge of that other person commits an offence'.

Similarly, the Act also requires confidentiality in communicating HIV test results. It states "the results of an HIV test shall be confidential and shall be released only to the person tested."[753] In the same line, the law requires medical practitioners to observe confidentiality while handling medical information and documents. It states that "all health practitioners: workers, employers, recruitment agencies, insurance companies, data recorders, sign language interpreters, legal guardians, and other custodians of any medical records, files, data or test results shall observe confidentiality in the handling of all medical information and documents particularly the identity and status of persons living with HIV and AIDS."[754] The major limitation of the Act is the fact that it protects privacy in the context of HIV and AIDS only.

Similarly, Human DNA Regulation Act, 2009 is another piece of legislation with some provisions regulating privacy right in the country. It provides for collecting, packing, storing, transporting, analysing and disposal of human DNA samples.[755] Moreover, it regulates the disclosure of all genetic information, access to genetic records, confidentiality, and research of the same in Tanzania.[756]However, privacy protection accorded by these few provisions of the Human DNA Act, 2009 are unlikely to be adequate in protecting privacy right in a setting where the protection of the right to privacy generally is missing such as in the cloud.[757]

Additionally, the Medical Practitioners and Dentist Act, Cap 152, of 2002 is also a

[753]The HIV and AIDS (Prevention and Control), 2008. Section 16 (1).
[754] Ibid, section 17 (1).
[755]The Human DNA Act, 2009, Section 23-37.
[756] Ibid, section 52-65.
[757]Ubena, J., Privacy: *A Forgotten Right in Tanzania*, the Tanzania Lawyer, 2012, Vol.1, No.2, pp. 72-114.

piece of legislation in the health sector with some implication for protecting privacy right. Under this Act, Code of Ethics and Professional Conduct for Medical and Dental Practitioners in Tanzania, was established in 2005. It provides for different principles and two among them are important for the protection of privacy right. Autonomy (self-determination) is the first principle, which requires inter alia that health practitioners should offer treatment and other forms of health interventions to a patient only when he or she gives an informed consent. Privacy is the second principle. This advocates that any information about a patient is private property, i.e. records, interests,the body (corpus) of the patient and all the affairs relating to the patient's conditions. The information should thus be restricted to the medical practitioner only.

5.2.5 Privacy Protection and National Security Sector

Despite the constitutional protection of privacy right in Tanzania under Article 16 (1), the same Constitution under Article 16(2) provides for a leeway of other pieces of legislation to impinge privacy right. According to the article, the law marker may enact a law to provide on how the right to privacy may be protected, pursued, or intruded by government authorities and its agents.[758]As a result, there are some laws in place with some inferences to privacy protection. These laws fall under peace and security sector. We discuss them in the subsequent paragraphs.

The first of these laws is Prevention of Terrorism Act. This is an Act, which was

[758]The Constitution of the United Republic of Tanzania, 1977. Article 16(2), It provides that '…For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.

enacted in 2002 to provide for comprehensive measures of dealing with terrorism, to prevent and to cooperate with other states in the suppression of terrorism and to provide for related matters.[759]The Act authorises police officers responsible with terrorism offences investigation to intercept communication.[760] However, the law requires the interference with someone's privacy to be lawful. The interception is regarded to be lawful only if before the interception, the officer applies "*ex parte*" to the High Court of Tanzania and acquires warrant authorising interception.[761]

Moreover, the law requires the police officer to make an application for the communication interception order after Attorney General Consent is granted.[762]After the application, if the Court satisfies itself that there are judicious grounds to believe that some information that relates to the commission of terrorism offence or about a person suspected of committing a terrorist offence is in the communication communicated or about to be communicated, the Court may order the service provider to intercept and retain that particular communications.[763]Conversely, the Court can issue an order authorising the officers of the police force to enter premises and install devices for intercepting and retaining of such particular communications, and afterwards to remove and retain the devices.[764]

However, the Act does not provide for the limitation period of the order that the Court may issue. This may result in the continuous interception of the targeted persons'

[759] Act, No. 21 of 2002.
[760] Section 31, Prevention of Terrorism Act, 2002.
[761] Ibid, section 31(1).
[762] Ibid, section 31 (2).
[763] Ibid, Section 31 (3), (a).
[764]Ibid, Section 31 (3), (b).

communication under the umbrella of the Courts' authorisation. This is applicable even if the investigation does not link the targeted person to the suspected offence. In the same vein, the Act does not provide for the erasure or deletion of the tapped communication, if it is not satisfactory enough to warrant prosecution of the suspected individual. Principally, from the gaps discussed above, though the Act seems to have met the procedural requirements as provided under Article 16 (2) of the Constitution of Tanzania, it is uncertain if it passes the proportionality test as provided under Article 30 (2) of the same Constitution.

Tanzania Intelligence and Security Act, 1996 is another legislation with an implication to privacy protection. This Act allows interception of private communication for the sake of state security.[765] The Act authorises Tanzania Intelligence and Security Service (TISS) to investigate any individual or a body of persons if it has any probable cause to consider him or her a risk or a cause of risk of a threat to the state security.[766]

Besides, according to this Act, TISS has the power to institute surveillance of some individuals or a category of individuals.[767] It is important to underscore that this Act defines the term intercept in relation to any communication lawfully obtained by the person making the interception to include hearing, listening to, recording, monitoring, or acquiring the communication, or acquiring its substance, meaning or purport.[768]More so, the term intercept has the same meaning with the term

[765] Cap 406, R. E. 2002.
[766] Ibid, section 15(1).
[767] Ibid, section 5(1), (d) and (2), (d).
[768] Ibid section 3.

interception.[769] However, the term intercept is found only at the definition section but not in the provisions provided for in the Act.

Similarly, it is important to highlight that the Act uses the term surveillance instead of the term interception, though the term surveillance is not defined in the Act. Principally, although the Tanzania Intelligence and Security Act, 1996 evaded the use of the term interception, it authorises, its uses in disguise of the term surveillance. It is worth noting that though the Act provides for surveillance and interception, it defines the grounds that authorise its uses very loosely and broadly.[770] It merely mentions state security as a blanket reason for interception and surveillance. Likewise, the Act does not provide for the procedures for surveillance and interception. As a result, the surveillance and interception are conducted without the need of a warrant or any prior authorisation. This implies that TISS Act when weighed against the Constitutional right of privacy as provided under Article 16, falls far below the mark of privacy protection accorded by the Constitution.

Furthermore, the Cyber Crime Act, 2015 is another law, which has some elements of privacy protection in Tanzania. The Act was made to protect information stored in the computer, and these may include personal information. Section 4 of the Act states:

(1) "a person shall not intentionally and unlawfully access and cause a computer system to be accessed.

(2) a person who contravenes subsection one commits an offence……."

[769] Ibid.
[770]Makulilo, note 716, supra.

Moreover, section 7 of the same Act states:

"a person who intentionally and unlawfully damages or deteriorates computer data, deletes computer data, alters computer data and renders computer data meaningless, useless or ineffective, commits an offence……."

The above provision simply that the Act criminalise unlawfully access to computer and hence provides protection to any data stored in the computer network. Similarly, it also criminalises any act, which constitutes illegal data interference. However, despite the fact that the Act purports to protect all the data stored in the computer, personal data inclusive, these provisions are very broad and widely constructed. Indeed, they do not specifically protect privacy of the personal data stored in the cloud. Consequently, privacy protection provided by this Act, when measured against the constitutional privacy stated in the constitution, is unsatisfactory.

Equally, the Registration and Identification of Persons Act, is another law in Tanzania with some implication to privacy protection.[771]The Act in intended to regulate all the matters relating to registration of persons and the issuance of national identity cards (National IDs) in the country. Since 2011, all Tanzanian citizens and residents are being registered and furnished with national IDs under this law. Among other things, the law prohibits the disclosure of information that is collected from different persons for registration purposes except in specific situations stipulated by the same law. This is clearly provided for under Section 19 which states:

"subject to section 18, the Registrar and any registration officer and any immigration officer performing functions under this Act shall not-

[771]Cap 36, R. E. 2002.

(a) produce for inspection, or supply a copy of, the photograph of any person registered under this Act or his fingerprints, or
(b) disclose or supply a copy of the particulars furnished under section 7 or 9, except and unless with the written permission of the Minister which may-
(i) refer to a person or category of persons by name, office or description; and
(ii) contain such terms and conditions as the Minister may deem fit to impose."

The disclosure provisions above seem to be protecting privacy and personal data. However, vesting the discretionary powers over personal data upon the Minister makes the provision to be very widely and broadly constructed. This is because the Act is silent on how the Minister's discretion powers can be checked against any probable abuse. In the same vein, the law on registration and identification of persons becomes uncertain by leaving the task of imposing the terms and conditions on each case on its own merit that would necessitate disclosure at the discretion of the Minister. Even more, the discretionary powers vested to the Minister lacks proper safeguards and controls that could enhance the protection of personal data in the database of the National ID Authority. This implies privacy protection as provided in this Act, is still at infancy stage when measured against the Constitution.

5.3 Conclusion

In summing up this part, it is imperative to highlight that there is no data privacy regulation in Tanzania, regardless of the fact that it is a member of the AU, SADC and EAC, which are the regional and sub-regional groups with some initiatives for data privacy protection. It is also absurd to find that there are no general public or parliamentary debates and discussions with the ultimate goal of adopting an omnibus data protection law. Further, it is worth noting that regardless of coming into force of the GDPR in May 25, 2018, the government has not felt the compulsion brought by

the requirement of Article 45 of the GDPR, to ensure an adequate level of protection of personal information in its domestic legislation. Probably, the exceptions stated in Article 49 of the GDPR are working efficiently for Tanzania at present.

Moreover, the presented analysis and examination of privacy and security issues in the cloud in Tanzania has revealed the lack of data privacy law to protect privacy and security in the cloud regardless of a constitutional right to privacy. Feeble protection provided by the constitution and the sectoral laws fall short of expansively protecting privacy in the cloud. Cloud computing technology being a new paradigm post-dates the constitution as well as sectoral laws with the elements of protecting privacy. As such, there is the need for a legislation that is tailored for privacy in the cloud for Tanzania.

CHAPTER SIX

PRIVACY AND SECURITY PROTECTION REGULATION IN THE CLOUD IN SOUTHAFRICA

6.1 Introduction

South Africa is regarded as one of the major ICT markets in African continent by value.[772] It demonstrates technological headship in the mobile software category, electronic banking amenities and security software.[773] Moreover, the general adoption rate of cloud computing services has increased; and South Africa now is considered a cloud evolving territory.[774] It is also regarded as a cloud computing technology hub, which is very important for access for sub-Saharan countries.[775] However, the degree of cloud computing adoption is low compared to the expectation due to a variety of constraining factors and trepidations that lead to the mistrust of the cloud.[776]

Major concerns identified are privacy and security in the cloud environment.[777] This chapter offers an outline of the context of cloud computing in South Africa, and assesses how it is regulated. It also provides an overview of the development of privacy legislation in the country. At the same time, it evaluates whether the existing privacy regulation is tailored to address cloud-computing technology. The strengths and the weaknesses of the current privacy regulation are provided as justification for

[772]The Department of Communications in South Africa, South Africa Information Technology, 2018. Accessed from https://www.export.gov/article?id=South-Africa-information-technology, Accessed on 7th January 2019.
[773] Ibid.
[774]Crowe, D., Cloud Adoption in South Africa. 2017. Accessed from https://www.shapeblue.com/cloud-adoption-in-south-africa/ on 7th January 2019.
[775] Ibid.
[776]Skolmen, note 52, supra.
[777] Ibid.

proposing the quick coming into force of a robust omnibus data protection law in South Africa.

6.2 Context of Cloud Computing in South Africa

Cloud computing is a new paradigm in computing technologies and is at present extensively accepted and used worldwide for its numerous benefits.[778]In recent years, migrating to the cloud has become prevalent all over the world due to its capacity, efficiency, cost effectiveness and simplified access.[779]Gillwald and Moyo are of the view that provision of cloud computing services in most of the African states is supply oriented especially in public sector rather than demand oriented.[780] However, South Africa seems to be an exceptional case because its adoption of cloud computing is demand driven through corporate sector.[781]

Putting it differently, one can say that demand of cloud service from private sector in South Africa stimulates the growth of cloud computing and technology is expansively used all over the nation.[782]It is used in private and public sector including e-government as well.[783] Currently, cloud computing global players, including the Microsoft, AWS and Google, are operating in south Africa. Google and Microsoft are

[778]Gebers, J., &Ophoff, J., Exploring Cloud Computing Legal & Privacy Issues in South Africa. A Conference Paper Presented in World Wide Web Applications Conference in Cape Town, on 10th to 13th September 2013. Accessed from https://www.academia.edu/Exploring_cloud_computing_legal_and_privacy_issues_in_south_africa, on 9th January 2019.

[779]Mzekandaba, S., Security Concerns Hold Back South Africa Cloud Adoption. 2014 Accessed from Http://www.itwebafrica.com/m/news/A69k9JN8V7nd, on 9th January 2019.

[780]Gillwald, A, et.al., note 70, supra.

[781]Ibid.

[782]Ibid.

[783]Mvelase, P. *et.al.* Towards a Government Public Cloud Model: The Case of South Africa. A Conference Paper presented in the Second International Conference on "Cluster Computing "in L'viv, Ukraine on 3rd to 5th June 2013. Accessed from https://www.researchgate.net/publication/237077704_Towards_a_Government_Public_Cloud_Model_The_Case_of_South_Africa, on 10th January 2019.

ambitiously marketing cloud computing services while competing with local companies like Internet Solutions. At the same time, the AWS provides massive shared computing capacity while competing with local establishment such as the MTN, Telkom, and Internet Solutions respectively.[784] Due to security and data protection concerns, cloud type preferred in South Africa is private cloud.[785] Nevertheless, many companies are migrating to public cloud so as to get the benefit of the economies of scale.[786]

It is worth highlighting that cloud computing is regarded as an extension of hosting and data centres, and hence a logical next step up the value chain.[787] It is remarkable that cloud computing in South Africa is applicable in health sector and is progressively gaining acceptance as an effective way of enlightening health care delivery.[788]. Despite the enormous benefits of cloud computing that fuel its acceptance, cloud technology and architecture give rise to inherent legal and regulatory concerns. This is because cloud computing generally shifts the data beyond the physical borders of the company. Consequently, issues such as privacy and security of data arises.[789] The privacy and security issues calls for regulatory intervention for cloud computing. The

---

[784]Gillwald, A., & Moyo, M. Prospects, Challenges and Impacts of Cloud: Perspectives from (South) Africa. A Presentation to UNCTAD Workshop on Cloud Economy, Geneva, February 2013. Accessed from https://researchictafrica.net/research/research-presentations, on 10th January 2019.

[785] Ibid.

[786] Ibid.

[787]Gillwald, et al., Understanding what is happening in ICT in South Africa-a Supply- and demand - side analysis of the ICT sector, 2012. Accessed from http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_7_-_Understanding_what_is_happening_in_ICT_in_South_Africa.pdf, on 10th January 2019.

[788]Mgonzi, T., & Weeks, R., The Impact of Cloud Computing on the Transformation of Healthcare System in South Africa. A Conference Paper Presented in 2015 ITU Kaleidoscope: Trust in the Information Society. Accessed from http://www.researchgate.net/publication/304295616_The_impact_of_cloud_computing_on_the_transformation_of_healthcare, on 10th January 2019.

[789] Sotto, L., *et. al*, Privacy and Data Security Risks in Cloud Computing, 2010. Electronic Commerce & Law Report.

following part provides an assessment of how security and data privacy is regulated in the cloud in South Africa.

6.3 Regulation of Cloud Computing in South Africa

Despite the fact that South Africa is regarded as cloud evolving nation and the ICT hub for sub-Saharan Africa, cloud computing is not systematically regulated. This implies that there is no sector specific regulation for Cloud Computing, and the existing data protection law (POPI) suffers some limitations in protecting security and privacy of data in the cloud.[790]Jaeger is of the view that there are some key issues in cloud computing which needs regulation.[791] These include privacy and personal data, anonymization, government surveillance, and telecommunication capacity.[792] Moreover, Muyinga, establishes that regulating cloud computing in South Africa among other things, implies regulating privacy.[793] The need of privacy regulation is evidenced by low adoption rate of cloud computing.[794] Putting it differently, privacy and security issues in South Africa leads to low cloud adoption rate, hence there is the need for privacy regulation so as to cure the anomaly.

In spite of not having a sector specific regulation for privacy in cloud environment in South Africa, still privacy is to some extent protected through general laws and

[790]Crowe, note 784, supra.
[791]Jaeger, P., T., et al., *Cloud Computing and Information Policy: Computing in a Policy Cloud*. Journal of information Technology and Politics, 2008: 5: 209-283.
[792]Ibid.
[793]Muyinga, M., Privacy and Legal Issues in Cloud Computing. The SMME Position in South Africa. A Conference Paper presented in the 11th Australian Information Security Management Conference, Edith Cowen University Perth, Western Australia on 2nd to 4th December 2013. Accessed from http://www.ro.edu.au/ism/156, on 10th January 2019.
[794] Ibid.

statutes.[795] The general law includes the South African Constitution and the common law, while, the statutes are sector specific in nature.[796] Arguably, privacy protection provided by those sources is not considered as satisfactory as the one accorded by the data privacy legislation.[797] There are propositions that inadequacies and the limitation experienced to some extent necessitated the adoption of an omnibus data privacy law known as Protection of Personal Information Act 4 of 2013. Nevertheless, since its adoption in November 2013 to date, it has not come into force, except for some few provisions that are intended to establish the office of the regulator.[798] This part assesses the responsibilities of the above-named sources in data privacy in South Africa. It also demonstrates strengths or weaknesses of the sources in data protection. It worth noting that more emphasis has been placed on Protection of Personal Information Act 4 of 2013, because it is an omnibus data protection law that awaits full implementation in a near, but unknown future.

6.3.1The Constitution of South Africa 1996

South Africa protects privacy as a constitutional right. Since the coming into force of the Interim Constitution in 1994, this right has been protected as a fundamental right.[799] Article 13 of the Interim Constitution stated that, 'every person shall have the right to his or her personal privacy, which shall include the right not to be subject to

[795]Burchel, J., *The Legal Protection of Privacy in South Africa: A Transplantable Hybrid*. Electronic Journal of Comparative Law, 2009, Vol 13.1. Accessed from http://www.ejcl/org/131/art131-2.pdf, on 10th January 2019.
[796]Gebers, note 778, supra.
[797]Makulilo, note 770, supra.
[798]The Government Gazette 37544 of April 11, 2014 the following sections came into force: s 1 (definitions); Part A of Chapter 5(establishments of Information Regulator); S 112 (grants the Minister the authority to adopt regulations); s 113 (procedures for making regulations), in Roos, A., *Data Protection Law in South Africa*, in Makulilo, A. B. (ed) African Data Privacy Laws, Switzerland, Springer International Publishing AG, 2016, pp. 189-228.
[799]Roos, A., Data Protection in Dana, M., *et al*. (2008) Information and Technology Law. LexisNexis, Durban, 2008, pp 313-392, at p 360.

searches of his or her person, home or property, the seizure of private possessions or the violation of private communications'.[800]Moreover, the same provision is reproduced in the final Constitution of South Africa in Article 14, which states that:

'Everyone has the right to privacy, which includes the right not to have-

(a) their person or home searched;

(b) their property searched;

(c) their possession seized;

(d) the privacy of their communications infringed.'[801]

The scope of protection that the article above provides is evidently narrow. The reason for this is that it warrants only a general right to privacy coupled with explicit protection against searches, seizures as well as communication infringement.[802] Nevertheless, there are arguments that the listing of privacy situations bequeathed in Article 14 is not comprehensive. Consequently, the protection accorded under this article is extending to other methods of collecting information or making unlawful disclosure.[803]

Moreover, although privacy instances reckoned in Article 14 of the South African Constitution refers to information aspect of the privacy right, the Constitutional Court has extended it to substantive privacy rights.[804] These are rights which empower an

[800]The interim constitution is the constitution towards the majority rule in South Africa, which marked the end of apartheid era. It was assented on 25th January 1994 and commence to apply on April 1994, Act 200 of 1994.
[801]The Constitution of the Republic of South Africa, 1996.
[802]Roos, note 799, supra.
[803]McQupid-Mason, D., J., Privacy in Chaskalson, M., et al (eds) Constitutional Law of South Africa, JUTA, Kenwny, 1996. Cited in Makulilo A., B., p 396, note 797 supra.
[804]*De Reuck v Director of Public Prosecutions, Witwatersrand Local Division* 2005 (1) SA 406 (CC).

individual to make decisions about their home, sexual life, and family in general.[805] In *Mistry v Interim Medical and Dental Council of South Africa*, the Constitutional Court of South Africa established some principles or factors to be considered in assessing whether the violation of the information aspect of privacy right has occurred.[806] These include the manner through which information was collected, whether intrusive or not, the nature of the information, whether intimate information or not, the initial purpose of collection, the manner and nature of the dissemination (to whom and how the information is communicated).[807]

As well, the decision of cases such as *Media 24 (Pty) Ltd and other v Department of Public works and others,*[808] *and Craig smith and Associates v Minister of Home Affairs and others,*[809]the Constitutional Court stated that in establishing whether the right to privacy has been violated or not, the right to privacy should be assessed against all other contending interests. However, in *Minister of Police and Others v Kunjana* the Court took a different stance but with the same intention of protecting privacy right. It stated that warrant less searches conducted by police officials in terms of the Drugs and Drug Trafficking Act 140 of 1992, where no urgency exists, breaches the right to

[805]Neethling, J., *et al*., Neethling's Law of Personality. 2nd ed, LexisNexis, Durban. 2005.

[806]1998 (4) SA 1127 (CC) 1145. See also Ross, A., *Data Privacy Law*, pp 363-487 in Van der Merwe, D., et al, Information and Communications Technology Law, 2016, at p 417.

[807]Ross, note 802, supra.

[808]2016 (3) ALL SA 870 (KZP). In this case the applicants were media houses who sought access to the disciplinary proceedings instituted by the first respondent against eleven of his employees in relation to the upgrades made to the President's Nkandala residence. The Court had to weigh the applicants right to freedom of expression against the privacy rights of the respondent and its employees. The court held that the right to freedom of expression, in this particular instance was a justifiable limitation placed on the right to privacy.

[809]2015 (1) BCLR 81 (WCC). The applicants in this case were a law firm suspected of committing fraudulent activities and the respondents were acting based on warrants obtained to search the applicant's premises for evidence in that regard. It was held that the applicant's right to privacy had to be weighed against the respondents right to search and seize evidence. An orderwas crafted to allow the applicants premises to be searched in compliance with their right to privacy which simultaneously satisfied the need for justice.

privacy of an individual and accordingly declared Section 11(1)(a) and (g) of the Act to be unconstitutional.[810]These decisions clearly cement the concept that privacy right is jealously protected by the Constitution and the court and hence, is not to be overridden in the absence of proper justification.[811]

Correspondingly, the constitutional right of privacy as provided in South African Constitution is considered as right that lies in the continuum state by the Constitutional Court.[812]This is to the effect that personal intimate domain is afforded higher level of protection while as an individual moves away from the most intimate domain he or she receives less privacy protection.[813]Moreover, the courts uphold the constitutional right of privacy by extending the aspects of human life in which an individual has a legitimate anticipation of privacy.[814]This was established in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smith*[815] where the court stated that wherever an individual has a capability to choose what he or she wishes to reveal to the general public, with reasonable expectation that the same will be respected, the right to privacy is invoked.

Nevertheless, privacy right as protected in the South African Constitution is argued to be very comprehensive. First and foremost is the phrase "everyone" which introduces

[810]2016 (9) BCLR 1237 (CC).
[811]Rasool, Y., An Examination of how the Protection of Personal Information Act 4 of 2013 (POPI) will Impact on Direct Marketing and the Current Legislative Framework in South Africa. Masters of Laws Dissertation submitted at University of Kwazulu-Natal, 2017. Accessed from http://www.researchspace.ukzn.ac.za/xmului/handle/10413/15029, on 11th January 2019.
[812]Ibid.
[813]*Bernstein v Bester NO*1996 (2) SA 751 (CC*).*
[814]Ross, note 807, supra.
[815]2001 (1) SA 545 (CC) para 16.

Article 14 of the Constitution; it implies that privacy right protected through this article encompasses citizen as well as non-citizen of South Africa. The only prerequisite is the physical presence of an individual in South Africa. This is the analogous to the GDPR and its predecessor Directive 95/46/EC, whose applicability is tied to the physical presence in the European Union irrespective of residence, nationality, or the reason of being present in the union.[816]

Secondly, the constitutional right of privacy is regarded to be wide-ranging on the ground that it is applicable to both natural and juristic persons. Article 8(2) provides that a provision of the bill of rights binds a natural or a juristic person if, and to the extent that, it is applicable, considering the nature of the right and the nature of any duty imposed by their right.' This implies that data controllers who, in most cases, are corporations enjoy the protection of privacy right offered by Article 14 of the South African Constitution. Yet, privacy right attributed to juristic persons is limited by Article 8(4) of the South African Constitution when it provides that 'a juristic person is entitled to the rights in the bill of rights to the extent required by the nature of the rights and the nature of that juristic person.' This was also upheld by the Constitutional Court when it held that:

> *'Juristic persons are not bearers of human dignity. Their privacy rights, therefore, can never be as intense as those of human beings. However, this does not mean that juristic persons are not protected by the right to privacy. Exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society, with serious implications for the conduct of affairs.... '*[817]

[816]Gilliland, note 595, supra.
[817]Investigating Directorate Case, note 819, supra.

While there is a general argument that constitutional protection of privacy is not as effective as the one provided by the data protection laws, the recognition of privacy as part of the fundamental rights in South African Constitution serves a very important role.[818]First and foremost, it thwarts the executive and the legislature from enacting any law or taking any action which may infringe or limit privacy right unreasonably.[819]Secondly, it gives privacy a higher status above all other laws and court decisions, state actions and above the conduct of legal and natural person alike.[820] That said, it must be noted that constitutional protection of privacy does suffice in protecting privacy in the cloud.

6.3.2 Common Law

Common law is the foundation of privacy protection in South Africa.[821] Most of the South African scholars agree that today's privacy protection as accorded in the Constitution has its origin from the common law, though now it is codified and some amendments have been made.[822] By using the common law, the South African government recognises privacy as personality interest of individuals.[823] These interests are protected by granting individuals subjective or personal rights over such interests, and hence protected through the law of *delict*.[824]

[818]Gorska, Z., M., Privacy, Surveillance and HIV/AIDS in the Work Place: A South African Case Study. M. A. Thesis, University of Witwatersrand, Johannesburg, 2008, p. 36. Accessed from https://www.wiredspace.wits.ac.za/bitsrteam/handle/10539/6762/1.07.pdf on 11th January 2019.
[819] Neethling, note 805, supra. P. 17.
[820] Ibid. p. 75
[821]Makulilo, note 797, supra.
[822] Neethling, note 820, supra, see also Ross, note 814, supra.
[823] Burchell, note 795, supra.
[824]Loubser, M., et al, The Law of Delict in South Africa. Oxford University Press of Southern Africa, Cape Town, 2010.

The interests referred to above are non-patrimonial in nature, in the essence that they cannot occur separately from an individual.[825]In addition, various personality interests are recognised. These include but not limited to privacy, identity, body, good name, dignity, physical liberty, and feelings.[826] It is noteworthy that these personality interests originate from Roman law. In fact, they are the advancements of the expansive triad of Roman law, generally known as *corpus* (physical integrity), *fama* (good name) and lastly, *dignitas*(a collective term for all personality aspects apart from *fama* and *corpus*.)[827]

Noteworthy, a *delict* is defined as an act of an individual that in an unjust or in the wrong way causes harm to another.[828] Generally, infringement of privacy occurs when true private facts of an individual are exposed to others against his or her will.[829] However, under the law of delict to succeed in a claim of privacy breach, five delict ingredients must be proved by the claimant. These include wrongfulness, act or conduct, causation, fault, and harm.[830]The contravention of a personal interest is regarded as an *iniuria* and the loss is only recovered through instituting the *actioiniuriarum*.[831] Moreover, the institution of *actioiniuriarum* is justified by the intentional breach of the personality interest in a wrongful manner.[832]Judging the conduct in question according to *boni mores* standard is the only means of establishing

[825] Neethling, note 820, supra.
[826] Ibid.
[827]Roos, note 814, supra.
[828]Neethling, J, et al, Neethling-Potgieter-Visser Law of Delict, 6th Edition, LexisNexis, Durban, 2010.
[829] Ibid, p, 347.
[830] Ibid.
[831]The Roman law concerning liability for injury to personality has been adopted in South Africa. See Neethling, *et al.*, Law of Delict, 7th ed, 2015, p 12.
[832]Roos, note 827, supra.

the wrongfulness.[833] Any conduct that is proved to be unreasonable against the *boni mores* standard is established as wrong. As a result, violation of any subjective right such as privacy right is regarded as an unreasonable and hence wrongful.[834]

Equally, the law of delict just like the English common law seeks to compensate the injured party for the harm caused, though this is not the only function.[835] However, under the law of delict, liability is established using general principles while the English law focuses on specific torts.[836]Arguably, the law of delict is more flexible than the English common law on the ground that it can accommodate varying situations and new emerging circumstances without establishing new delicts, which is a long, slow, and cumbersome legislative process.[837] As a result of its flexibility, the law of delict recognises and protects personal interests including but not limited to privacy and goodwill of even cooperation, which are created in post-modern era.[838]

Notably, the processing of personal data threatens personality interests of individuals such as privacy and identity.[839]Accordingly, in *Jansen van Vuuren v Kruger,* the Constitutional Court established that the *actioiniuriarum* (a legal action for violation of a personal interest) protects a person's *dignitas*.[840] This implies that these personality interests are regarded as part of the *dignitas* concept.[841] As alluded to, privacy is breached when true personal data are processed, while identity is said to be

[833] Ibid.
[834]Neethling, note 828, supra.
[835]Neethling, note 825 supra.
[836]Van der Walt & Midgley. J., R., Principles of Delict, Butterworths, South Africa, 2005, P 31.
[837]Ibid.
[838] Neethling, note 835, supra.
[839]Neethling, note 834, supra.
[840]1993(4) SA 842(A), p.849.
[841]Roos, note 832, supra.

infringed if personal data processed happen to be untrue.[842]Moreover, personality interests of privacy and identity are also recognised in case law. This was clearly shown in *O'Keefe v Argus Printing & Publishing Co Ltd*[843]a landmark case that established that privacy right is a recognised in South African common law.

Similarly, *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*[844] is classical case that recognised identity as an independent right to be protected for the first time. The same was recognised in *Grutter v Lombard*.[845] In addition, the common law as practiced in South Africa protects some personality rights attributed to the juristic persons in line with the Constitution. These include the right to identity, good name, and privacy.[846] Regardless of the general understanding that privacy is protected through common law in South Africa, the protection provided by the law of delict is too broad. Its applicability is extended to every individual who resides in South Africa regardless of their citizenship.[847] Moreover, the protection afforded by the traditional common law principles is not applicable to legal challenges and issues created by the processing of personal data in more advanced technology such as cloud computing.[848] Notably, it lacks data protection principles.[849]

6.3.3 Statute Law

Prior to the adoption of the Protection of Personal Information Act (POPI Act) in 2013,

[842]Ibid.
[843]1954(3) SA 244(C).
[844]1977(4) SA 376 (T) 386.
[845]2007 (4) SA 89 (SCA).
[846]A juristic person does not have personality rights that involve the feelings of a person such as dignity or the body of a person (physical integrity). Neethling, et al, note 839, supra.
[847]Ross, note 9, supra. p 590 Cited in Makulilo, (LL. D Thesis) note 821, supra.
[848]Neethling, et al, note 839, supra.
[849]Ibid.

South Africa did not have omnibus data protection legislation.[850] Even, the promulgation of POPI Act did not bring gigantic changes on data privacy protection due to the fact that only few sections of the Act have come into force to date.[851] As a result, privacy in South Africa is still protected through the common law, Constitution and some sectoral laws containing some data protection provisions, as pointed above. Notwithstanding, the current protection is inadequate in the light of data protection laws. These statutes are discussed hereunder clusters of financial sectors, health sector and communication sector. It is worth noting that more emphasis is on the Protection of Personal Information Act, 2013.

6.3.3.1Security and Privacy Protection in Financial Sector

Information technology and commercial activities are becoming inseparably interwoven to the extent that business that falls short of some level of technical savvy is probable going to fail.[852] Information technology brings enormous benefits in businesses. Meanwhile, it is a fertile ground for threat to privacy and data protection in the absence of robust data protection regulation. In this realization, South Africa has some laws in financial sector for protecting privacy. Consumer Protection Act (CPA) is one of such laws.[853]This Act protects privacy and confidentiality of individuals in respect to unsolicited or unwanted communication.[854] It gives the

[850]Naude, A., Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Development. LL. M. Mini Dissertation, University of Pretoria, 2014. Accessed from http://www.repository.up.ac.za/bitstream/handle/2263/46094/Naude_Data_2015_pdf.
[851]Ross, note 841, supra.
[852]Emma, L., Importance of Technology in the workplace,2018. Accessed from http://www.smallbusiness.chro.com/importance-technology-workplace-10607.html, on 12th January 2019.
[853] Act No 68 of 2008 accessed from https://www.gov.za/documents/consumer-protection-act, on 13th January 2019.
[854] Ibid, section 11.

customer the right to refuse unsolicited telephone calls, spam emails, messages, and letters.[855]

Correspondingly, the National Credit Act (NCA) is another law, which contains some provisions that protects privacy under commercial sector.[856]The Act protects privacy by the provision which stipulates that organisations/entities or persons who compile, retain, report, or receive confidential information about individuals should protect that information.[857] In doing so, they must use that information only for the purposes in which the consumer consented or the ones authorised by the law.[858] The Act further states that an entity or persons holding confidential personal information of the customers may release the information only under the order of the court or with the authorisation of the customer.[859]

In addition, the Act provides for the right to access and challenge credit records information.[860]This implies that the consumer has the right to access the information about himself or herself that is in the custody of the credit bureau and challenge or request the proof of its accuracy.[861] The law compels the credit bureau to provide the proof of accuracy and to remove the disputed data from the records if it fails.[862] In the same vein, the Code of Banking Practice issued by the Banking Association in South Africa, the financial Advisory and Intermediary Services Act provides for similar

[855] Ibid.
[856] Act No 34 of 2005.
[857] Ibid, section 68.
[858] Ibid.
[859] Ibid, section 1, defines "confidential information as personal information that belongs to a person and is not generally available to or known to others".
[860]Ibid, section 72.
[861] Ibid.
[862] Ibid.

provisions requiring clients' personal data to be treated as confidential and as private as possible.[863] The only exception allowed is where there is a legal duty to disclose or to the protection of its interest.[864] Nevertheless, these Acts are limited in their protection of privacy considering that they only apply to the specific sector.

6.3.3.2 Security and Privacy Protection in Health Sector

Health sector is among the sectors where protection of privacy is crucial. Consequently, the National Health Act of South Africa has some provisions for privacy protection (albeit limited).[865] The Act requires that all information relating to health status, types of treatment and stays in a health establishment of the patient to kept confidential.[866] It prohibits any disclosure of personal data by the medical personnel except with explicitly written consent of the patient, or under the compulsion of the law or order of the court or if the information represents a serious threat to public health.[867] The Act also criminalises failure in protecting health records, which leads to divulgences of information.[868]Besides, the Children's' Act[869]and the Choice on Termination of Pregnancy Act,[870] contain some provisions which provide for the confidentiality of information, though in limited circumstances. Nevertheless, the provision applies only to privacy protection in health sector and does not have the general application.

---

[863]Issacs, R, *et al*., Data Protection Law in South Africa: Overview, 2018. Accessed from http://www.uk.practicallaw.thomsonreuters.com/5-5003-0787, 0n 15th January 2019.
[864] Ibid.
[865] Act No 61 of 2003. Accessed from http://www.gov.za/documents/national-health-act-pdf, on 16th January 2019.
[866] Section 14 (1), ibid.
[867]Section 14 (2), ibid.
[868] Section 17. Ibid.
[869] Section 13 (d), Act no 38 of 2005.
[870] Act no 92 of 1996.

6.3.3.3 Security and Privacy Protection in Communication Sector

As alluded to, privacy is protected through some sector specific laws in communication sector too (albeit limited). Promotion of Access to information Act (PAIA) is one of those laws.[871] This Act was enacted with the intention of giving effect to the constitutional right of access to any personal information in the custody of public or private sector.[872] The Act provides for the protection of privacy by addressing some general data protection principles.[873] First, it provides that individuals should have an access to information records, which contain information about them in both private and public bodies, personal information inclusive.[874]Equally, the Act prohibits disclosure of personal information records if it will lead to an unreasonable disclosure of the information relating to a third party.[875] However, the Act applies only to access of information and prohibition of disclosure in some situations only.

Similarly, Electronic Communication Act (ECA) is another Act providing for data protection.[876] It is a law regulating among other things all telecommunication service providers. The Act requires all telecommunication service providers to be licensed. Moreover, the Electronic Communication Regulation obliges all licensed service providers to keep their clients' personal data confidential.[877] In addition, the Regulation of Interception of Communication and Provision of Communication-

[871] Act No 2 of 2000.
[872] Ibid, preamble of the Act.
[873] Naude, note 850, supra.
[874] PAIA, section 11.
[875] Ibid Section 34.
[876]Act no 36 of 2005. Accessed from https://www.gov.za/sites/default/files/gcis_document/201409/936-050.pdf, on 15th January 2019.
[877]Issacs, note 863, supra.

Related Information Act (RICA) provides for the protection of privacy.[878] The Act provides for the interception of communication as well as prohibiting telecommunication service providers from disclosing information obtained in the course of their work except in some exceptional circumstances as provided by the law.[879] The prohibition is applicable to both fixed line and mobile network operators. Indeed, the Acts are limited in their application as they are applicable to their respective assigned sector only. They have no general applicability.

In the same line, Electronic Communication and Transactions Act(ECTA) is another Act which protects privacy though in a limited way.[880]The Act regulates e-commerce in South Africa.[881]It is applicable only to personal data obtained through electronic transactions such as e-mail, internet, and short messages.[882]It governs a range of services such as e-government services, protection of personal information, consumer protection, electronic transactions, cryptography and authentication service providers.[883]

Chapter VII of the Act comprises two provisions which provide for data protection principles applicable to protect personal information in electronic transactions.[884]It

[878]Act no 70 of 2002. Accessed from https://www.justice.gov.za/legislation/acts/2002-070.pdf, on 15th January 2019.
[879]Section 42, ibid.
[880]Act no 25 of 2002.
[881]Michalsons, Guide to ECT Act in South Africa, 2018. Accessed from https://www.michalsons.com/blog/guide-to-the-ect-act/81, on 14th January 2019.
[882]Section 50 of ECTA.
[883]Muyinga, note 783, supra.
[884]Section 1 of ECTA provides a wide definition of the term transaction. It means "a transaction either of a commercial or non-commercial nature, and includes the provision of information and e-government services."

provides that personal data should be processed lawfully with the consent of the data subject.[885] It also advocates that personal data should be collected and processed for a lawful purpose only.[886] The law requires that data subject should be fully informed and hence knowledgeable of the purposes for which his or her personal data are being processed.[887] The law entails that if the data controller wants to process the data for any other purposes than the one consented to by the data subject, they should seek for consent again or do it under the compulsion of the law.[888]

In addition, the law requires the data controller to keep a record of the personal data and the specific reasons for data collection as long as the data are in use and one year thereafter.[889]Moreover, the law seeks to ensure that personal data in the custody of the data controller should not be disclosed to the third party without specific written permission from the data subject or unless permitted or required by the law.[890] In the same vein, the law requires that if the data were disclosed to a third party, the records of the third party and the dates of the disclosure to be kept as long as the data are in use and one year thereafter.[891] Similarly, the law entails the data controller to delete or destroy any personal data in his custody once they become obsolete.[892]In addition, ECTA provides for the principle of anonymity by allowing the data processor to

[885] Section 51 (1) of ECTA.
[886] Ibid, section 51(2).
[887] Ibid, section 51 (3).
[888] Ibid, section 51 (4).
[889] Ibid, Section 51(5).
[890] Ibid, section 51(6).
[891] Ibid, Section 51(7).
[892] Ibid, section 51(8).

compile profiles for statistical purposes but to make sure that profiles or statistical data cannot be linked to any data subject by the third party.[893]

Largely, the ECTA echoes the general data protection principles. However, the applicability of these principles in data protection in electronic transaction is voluntary. It entails that the data controller may subscribe to those principles by recording that fact in any agreement entered into with the data subject.[894] Moreover, if the data controller decides voluntarily to subscribe to the data protection principles, the law requires him or her to comply with all in its entirety.[895] Equally, in the event of breach of data protection principles, the rights and obligation of the parties are regulated by the terms of any agreement between them.[896]

Arguably, the voluntary nature of these principles is the glaring deficiency of the Act.[897] The same goes to the fact that the law does not establish a regulatory authority to oversee compliance. In addition, the Act is limited by the fact that it applies only to personal information collected through electronic transactions. Nevertheless, the provisions for data protection in the ECTA will be repealed as soon as the POPI Act comes into force.[898]

[893] Ibid, section 51(9).
[894] Ibid, section 50(2.)
[895] Ibid, section 50(3).
[896] Ibid, section 50(4)
[897] Naude, note 873, supra.
[898]Issacs, note 877, supra.

6.3.3.4The Protection of Personal Information Act of 2013

Almost forty years after the enactment of the first comprehensive national data privacy law in the world, South Africa adopted its own.[899]The shortcomings of the above-discussed statutory and general laws in South Africa necessitated an overhaul of the statutory framework so that the laws will provide acceptable level of data protection in the digital era.[900]Moreover, the pressure exerted by the EU through the then, EU Directive which obliged non-EU member states to adopt laws which are in compliance with the EU Directive and hence meet the EU adequacy standard, forced South Africa to enact specific privacy and data protection law.[901]The initiatives towards the enacting of this law were first taken by the South African Law Reform Commission (SALRC) in 2001.[902]

The first bill (the Protection of Personal Information Bill) was introduced in 2009.[903] Since the initiatives started, it took thirteen years until the Act was adopted.[904] It adopted an EU model of data privacy legislation.[905]The Protection of Personal Information Act (POPI), a comprehensive legislation regulating personal data in South Africa was signed into law in November, 2013.[906] April, 2014 is a noted date, in which

[899]Sweden enacted its first Data Act in 1973. In Greenleaf, G., Global Data Privacy Laws: Forty Years of Acceleration. Privacy Laws and Business International Report no 112, 2011, pp 11-17. Accessed from http://www.ssrn.com/abstract=1946700, on 16 January 2019.

[900]Naude, A &Papadopoulos, S., *Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments, (Part 1*), THRHR Journal, 2016, 51-68. Accessed from http://www.ssrn.com/abstract=2835387, on 17th January 2019.

[901] Article 25 and 26, Directive 95/46/EC.

[902] Ibid.

[903] Bill 9 of 2009, in Ross, note 851, supra.

[904] Ibid.

[905]Abdulrauf, L., A., Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa. LLD Dissertation, University of Pretoria, 2016, Pp 255.

[906] Act No 4 of 2013, in Issacs, note 898, supra.

few sections of the Act came into force.[907] These sections aimed at the establishing of the information regulators' office and issuing the Act's Regulation.[908] The office bearers were appointed and the information regulator assumed the office from 1st December 2016.[909] Moreover, the first of the draft regulations were issued in September 2017, and final regulations were published by the information regulator in September 2018, yet the Act did not come into force.[910]

Formerly, it was assumed that the POPI Act would come into force fully after the establishment of the office of the information regulator and the issuance of the regulation. Material aspects of the POPI Act are not yet enforceable and have no probable operative date. Arguably, as the long waited POPI regulations have been released, it is expected that the commencement date of the full Act will be announced soon. It is worth noting that once the Act enters into force, parties who process personal data will have a grace period of one year in which they are required to comply with provisions of the Act.[911]The rest of the chapter discusses the provisions of the Act. However, considering that the Act is voluminous only the most important aspects are going to be discussed. Further, reference to GDPR and its predecessor, the EU

[907]Pillay, L., South Africa: Data Protection Legislation, Hogan Lovells Global Media and Communications Quarterly, 2014. Accessed from http://www.lecology.com/library/detail/aspx.?g=09cbc4c1-1825-431e-b180-08e006ed2cb1, on 20th January 2019.

[908] According to the Government Gazette 37544 of 11th April 2014 the following sections came into force: sect 1 (definitions); Part A of Chapter 5 (establishment of information Regulator); Section 112 (grants the Minister the authority to adopt regulations); and sect 113 (procedures for marking regulations). In Ross, note 902, supra.

[909]Michalsons,Information Regulator in South Africa, 2017. Accessed form https://www.michalsons.com/blog/information-regulator-in-south-africa/13893, on 20th January 2019

[910]Vyver, et al, *POPI: Final Regulation Published*. South Africa Financial Regulation Journal, 2019. Accessed from https://www.financialregulationjournal.co.za/2019/01/24/popi-final-regulations-published, on 26 January 2019.

[911]Section 114 (1), POPI

Directive is made from time to time, because the two are the basis of POPI Act. Moreover, since the Act is yet to be fully implemented, no case law discussed in interpreting the Act.

First, the main objective of the POPI Act is to give effect of the constitutional right of privacy, by protecting personal information whenever it is processed by the data controller both in private or public sector and in line with international benchmark standards.[912]According to the Act, personal information implies any information relating to an identifiable, natural living person, and an identifiable, existing juristic person.[913] The Act also provides a list of information qualifying to be termed as personal information.[914] However, the list is not comprehensive to the effect that every case should be judged on its own merits. Notably, information such as genetic

[912]Act 4 of 2013, Section 2, the preamble of the Act provides for the purpose of the Act to include (a) giving effect to the Constitution right of privacy by safeguarding personal information when processed by a responsible part, subject to justifiable limitations that are aimed at (i) balancing the right to privacy against other rights, particularly the right to access of information and (ii) protecting important interests, including the free flow of information within the Republic and across international borders; (b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information; (c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and (d) establish voluntary and compulsory measures, including the establishment of an information Regulator, to ensure respect for and to promote and fulfil the rights protected by this Act.

[913]Section 1, ibid.

[914]Personal information includes (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of persons; (b) information relating to the education or the medical, financial, criminal or employment history of a person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of a person; (e) the personal opinions, views or preferences of the person; (f) correspondences sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the originalcorrespondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

information, the IP addresses and other information that closely relate to a person may also be considered as personal information.[915]It is worth noting that in defining the data subject, the Act includes the juristic person, which is contrary to the GDPR and its predecessor, the EU Directive (its model) and other international instruments.[916]

The scope of the Act is also very broad. That is applicable to both automated and non-automated processing of personal data that are entered into record by or for the responsible party (data controller) from either public or private sector as well.[917]It requires that if the processing is through non-automated means, it should form part of the filling system or it is intended to form part of it thereof.[918]Similarly, the term responsible party is also extensively defined to mean a public or private body or any other person which alone or in conjunction with others, determines the purpose of and means for processing personal information.[919]

Likewise, it applies to natural person and juristic persons as well.[920]Correspondingly, it is applicable only when the responsible party is a citizen of South Africa or non-citizen using equipment in South Africa.[921]However, the Act is not applicable if the data controller uses the equipment in South Africa just as a conduit for forwarding personal information through the country.[922]However, any processing of personal data in the course of a purely personal or domestic activity is not within the ambit of the

[915]Roos, note 861, supra.
[916]Ibid.
[917]POPI, Section 3 (1), (a).
[918]Ibid.
[919]Ibid, section 1.
[920]Ibid.
[921]Ibid, Section 3 (1), (5).
[922]Ibid.

Act.[923]

An example of this is when an individual collects and keeps telephone numbers and addresses of his friends then processes them for purely domestic or personal use, the risk posed to third parties privacy is very minimal hence it needs not to be regulated.[924]However, according to Ross, this exception is applicable only when the person collecting the personal data does not place it on the internet and expose or make it accessible to different people, other than his or her family.[925]

Correspondingly, processing of personal information that has been anonymised by eliminating any identifiable features (de-identified) to the extent that it cannot be linked to a certain individual again (re-identified) is excluded.[926]In addition, excluded from the application of the Act is the processing of personal data by or on behalf of the public body involving national security, defence, public safety of for the purpose of preventing and detecting an unlawful activities, combating money laundering, prosecution, and execution of sentences or security measures.[927] Nevertheless, the exclusion is allowable provided that respective laws regulating public bodies in those specific areas establishes adequate safeguards for the protection of such personal information.[928]

Additionally, any processing of personal data by the cabinet, its committees and the

[923] Ibid, section 6 (1), (a).
[924] Ross, note 916, supra. P 371.
[925] Ross, A., *Personal Data Protection in New Zealand: Lessons for South Africa*. Potchefstroom electronic Law Journal, 2008, vol 11, no 4, pp 61-109, at p 92. Accessed from https://www.ajol.info/index.php/pelj/article/view/42243, on 20th January 2019.
[926] POPI, section 6, (1), (b).
[927] Ibid, section 6 (1)(c).
[928] Ibid.

executive council of the province is excluded from the ambit of the Act.[929] The same applies to any processing of personal information by the court of law in the course of fulfilling its judicial functions.[930]Likewise, the Act excludes from its ambit the processing of personal data done exclusively for the journalistic, literary, or artistic expression purposes.[931] Yet, the exclusion is permissible to the extent that it is necessary to reconcile as a matter of public interest, the right to privacy with the right to freedom of expression.[932] Moreover, any processing of personal data that is in breach of the Act, which are exempted by the regulator subject to reasonable conditions are not within the ambit of the Act.[933]It is notable that most of the exemptions to the general rule in the POPI Act are fairly similar to those found in EU regulation.[934]

Arguably, the language used in Section 37 with the word "may" implies that the duty to publish the notice is not mandatory. The regulator may not publish the notice and yet be in compliance with the Act.[935] In addition, the section infers that it is wholly upon the regulator to determine the reasonable conditions in any particular case, and this does not provide proper safeguards. Moreover, it also implies that it is not obligatory to impose the reasonable conditions; the regulator is free to do it at his or her own discretion. It can be submitted that the exceptions provided under Section 36 and 37 of the Act in relation to the regulator's power to provide exception might not

[929] Ibid, section 6 (1), (d).
[930] Ibid, section 6 (1), (e).
[931] Ibid, section 7 (1).
[932] Ibid.
[933] Ibid, Section 37.
[934] Ross, note 925, supra.
[935]Makulilo, note 821 supra.

satisfy the data protection standard set in the GDPR, and hence negatively affect the general assessment of adequacy according to the GDPR standards.[936]

Similarly, the Act establishes the office of the information regulator, headed by a juristic person.[937]The Act also provides for the powers, duties and functions of the regulator, which includes providing education, monitoring and enforcing compliance, consulting with the interested parties, handling the complaints, researching on instruments relating to personal information of the data subject and reporting to the parliament and facilitating cross-border cooperation in enforcing privacy laws.[938]

The core of the Act is found in Chapter Three, where the eight conditions for lawfully processing of personal data are provided for. These conditions are imperative in any data protection instrument as they intend to ensure fair and lawful processing of personal data.[939]These conditions need to be viewed holistically due to the fact that they cannot stand in isolation and often times they interact and overlap with another.[940] The conditions are similar but not exactly identical to the data protection principles found in the Council of Europe Convention, the OECD guidelines and the GDPR.[941] Ross posits that POPI provides heightened protection for delicate or sensitive personal data, which are regarded as special personal information, and personal information of

[936]Ibid.
[937] POPI, section 39.
[938] Ibid, section 40.
[939]Abdulrauf, note 905, supra.
[940]Heyink, M., Protection of Personal Information for South African Law Firms. LSSA Guidelines, SALRC Report, 2011, p. 161. Accessed from http://www.jaa.org.za/doc-manager/protection-personal-information-law-firms-lssa-guidelines-2011, on 20th January 2019.
[941]Ross, note 934, supra.

children.[942] The conditions provided in the POPI for lawfully processing of personal data includes accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. Briefly, these are going to be discussed as follows:

Accountability is the first condition used as an umbrella to cover a myriad of responsibilities.[943] It requires the responsible party to ensure that all other conditions for the lawful processing of personal data provided in the Act are complied with.[944] It also specifies the time for its compliance, which is the time for determining the purpose and means of processing and during actual processing.[945] This section implies that compliance with these conditions is not intended to be done retrospectively. It is noteworthy that in terms of this condition, it is the responsible party who is eventually held responsible for compliance irrespective of whether the data were processed by the operator for or on behalf of the responsible party.[946] Furthermore, this condition seeks to strengthen trust in data processing environment and to empower the data subjects (individuals) to enforce their rights given that current data processing activities are conducted behind closed doors.[947]

---

[942] Ibid.

[943]Sloot, B., *Do Data Protection Rules Protect the Individuals and should They? An Assessment of the Proposed General Data Protection Regulation*. International Data Privacy Law, 2014, vol 4, Issue 4, pp. 307-325, at pg 309. Accessed from https://www.academic.oup.com/idpl/article-abstract/4/4/4307/2569055?, on 20th January 2019.

[944] POPI, section 8.

[945] Ibid.

[946]Heyink, note 940, supra.

[947]De Hert, P &Papakonstantinou, V., The Proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of Individuals. Computer Law & Security Review, 2012, vol 28, issue 2, pp 130-142. Accessed from https://www.sciencedirect.com/science/article/pii/S0267364912000295, on 1st February 2019.

Processing limitation is the second condition which upholds four aspects limiting the processing of personal data to assure that processing is done within the ambit of the law.[948] The first aspect entails that data processing should be done lawfully and reasonably, to the extent that it does not infringe privacy of the data subject.[949] The second aspect is minimalism, which intends to limit the processing of personal data to the purposes, which are adequate, relevant, and not excessive.[950] However, terms such as adequate, relevant, and not excessive are prone to different interpretations.[951] Yet they are not defined in the Act.

Consent, justification, and objection provide a third aspect of the processing limitation condition under the POPI Act. This is to the effect that processing of personal information is lawful only when there are grounds justifying the processing.[952] Consent of the data subject is part of the grounds mentioned above.[953] However, at any time, the data subject may withdraw his or her consent without affecting the lawfulness of the processing done before the withdrawal.[954] It is upon the responsible party to prove that the consent was given by the data subject.[955] Likewise, at any time,

---

[948] Neethling, J., *Features of the Protection of Personal information Bill, 2009 and the Law of Delict,* Journal of Contemporary Roman-Dutch Law, 2012, vol 75, pp241-255. Accesses from http://www.papers.ssrn.com/so13/cf_dev/AbsByAuth.cfm?per_id=1635090, on1st February 2019.

[949] POPI Act, Section 9.

[950] Section 10 ibid.

[951] Abdulrauf, note 939, supra.

[952] POPI Act, Section 11 provides for the grounds which makes the processing of personal data lawful. These includes a) that data subject or a competent person where the data subject is a child consents to the processing, b) Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party, c) Processing complies with an obligation imposed by law on the responsible party, d) Processing protects legitimate interest of the data subject. e) Processing is necessary for the proper performance of a public law duty by a public body, or f) Processing is necessary for pursuing the legitimate interests of the responsible party to whom the information is supplied.

[953] Section 1 defines consent as any voluntary specific and informed expression of will in terms of which permission is given for the processing of personal information.

[954] Section 11 (2) (b).

[955] Section 11 (2) (a).

the data subject may also object the processing of his personal information, unless the processing is under the compulsion of the law.[956] However, the objection must be on reasonable grounds.

Equally, the fourth aspect requires direct collection of personal information from the data subject.[957]According to Ross, this requirement is very crucial as it enables the data subject to be conversant with the processing of his or her personal data.[958]Nevertheless, this stringent requirement is subject to a list of exception especially for public and legitimate interest purposes, which ultimately dilute its effect considerably.[959]

The third condition is purpose specification. This requires that personal information should be collected for specific, explicitly defined and lawful purposes relating to the activities or functions of the responsible party.[960]This is an indispensable condition in privacy legislation as it determines the scope of data processing and underpinning all other aspects relating to data processing under the ambit of the Act.[961]Moreover, the Act obliges the responsible party to take reasonable measures to ensure that the data

[956] Section 11(3) (a).
[957] Section 12 (1).
[958] Ross, note 941, supra.
[959] POPI Act, Section 12 (2)(a)-(f) Provides some examples of situations in which information need not be collected directly from the data subject to include, when information is contained in or derived from a public record or has deliberately been made public by the data subject, data subject has consented to the collection of the information from another source, collection of the information from another source would not prejudice a legitimate interest of the data subject, or is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences, comply with obligation imposed by the law, in the interest of national security or compliance is not reasonable practicable in the circumstances of the particular case(to name but a few).
[960]POPI Act, Section 13.
[961] Neethling, note 948, supra.

subject is informed of the purpose when personal information is collected,[962] unless the former is exempted.[963]In the same vein, the condition requires that information should not be retained for a longer period than is required for realising the purpose for which it was collected and subsequently processed.[964] However, for research, historical, and statistical purposes, the condition allows the records to be kept for a longer period if there are appropriate safeguards in place.[965]

Further processing limitation is the fourth condition. This provides that any further processing of personal information should be compatible with the collection purposes.[966]It is submitted that further processing includes both the use and disclosure of personal information, and hence the applicability of this principle is more on use and disclosure of the collected information.[967] Compatibility is assessed by taking into account the relationship between the initial purpose of data collection and the purpose of the envisioned further processing, the nature of the information, the consequences of the further processing upon the data subject, the manner in which the information was collected and any contractual rights or obligations between the parties.[968]However, any further processing of personal data is not considered as

[962] Section 18(1)(a)–(h) requires the responsible party to ensure that that data subject is aware of the information being collected, the name and address of the responsible party, the purpose for which the information is being collected, whether the supply of the personal information by the data subject is voluntary or mandatory, the consequences of failure to provide the information, whether any particular law authorizes the collection of the personal information, the fact that the responsible party (where applicable) intends to transfer the personal information to another country and any other relevant information.
[963] Ibid, section 18 (4).
[964] Ibid, section 14 (1).
[965] Ibid, section 14 (2).
[966] Ibid, section 15 (1).
[967] South African Law Reform Commission (SALRC), Privacy and Data Protection Report, 2009, para 4.2.174. Accessed from http://www.justice.gov.za/salrc/dpaper/dp109.pdf, on2nd February 2019.
[968] POPI section 15(2).

incompatible with the initial purpose of collection if the data subject has consented the further processing. Also, if the information is a public record or is made public by the data subject himself or herself; further processing is necessary for national security, for court proceeding, maintenance of the law, and preventing a threat to health and if the information is used for research or statistical purposes.[969]

Information quality is the fifth condition. The condition entails the responsible party regarding the purposes for the collection and further processing of personal information to ensure that the information collected is complete, accurate, updated, and not misleading where necessary.[970] This condition has no exceptions and intends to obviate presenting misleading personal information, which may lead to discrimination or loss of benefits.[971]

Similarly, openness is the sixth condition. It requires the responsible part to keep a record of all processing operations under its responsibility.[972]It puts obligation upon the responsible part to ensure that the data subject is informed about collection of his personal data, collection source, the name and address of responsible party, the purpose of the collection and whether giving information is mandatory or voluntary. The information given to the data subject should contain the consequences in case of a failure in giving information of whether the collection of information is authorised by the law, whether the responsible party anticipates to transfer the personal

[969] Ibid, section 15(3).
[970] Ibid, section 16.
[971] Neethling, note 961, supra. Pp. 251-52.
[972] POPI Act, section 17.

information to a third country or international organisation and the level of protection. Moreover, responsible part is duty bound to provide any other relevant and necessary information that the data subject needs to know so that the processing of his or her personal data becomes reasonable.[973]

The seventh condition provides for security measures on integrity and confidentiality of personal information.[974] It obliges the responsible party to ensure that personal data under its custody and control are safe and secure. He or she is required to apply reasonable and appropriate technical and organisational measures to secure, not only the confidentiality, but also the integrity of personal data.[975] The information is protected against risks such as loss, destruction, unlawful access, or processing of personal information.[976]

Furthermore, identifying the risk, establishing the appropriate safeguards, maintaining them, verifying the implementation of the safeguard frequently, and updating the safeguards whenever necessary are among the specific measures to be taken by the responsible party while adhering to this condition.[977] Accordingly, if the operator processes information on behalf of the responsible party, he or she will do so under lawful authorisation of the responsible party.[978] The relationship between them is established by concluding a written contract with the effect that the latter ensures that the former establishes and maintains the security measures.[979]

---

[973] Ibid, section 18(a)-(h), then exceptions are listed in 18(4), (a)(f).
[974] Ibid, section 19.
[975] Ross, note 958, supra.
[976] POPI Act, section 19 (1).
[977] Ibid, section 19 (2).
[978] Ibid, section 20 (a).
[979] Ibid, Section 21 (1).

The processer is also obliged to ensure confidentiality of the information that comes to his or her knowledge.[980] Likewise, he or she is required to notify the responsible party, if the information is accessed or acquired by an unauthorised person.[981]In the same vein, the responsible party is required by the law to notify not only the regulator but also the data subject in case personal data have been accessed or acquired by unauthorised person.[982]This obligation is generally known as data breach notification; and it is among the contemporary features of data privacy laws.[983]

Data subject participation is the eighth condition, which gives the data subject active control over the processing of their personal information held by the responsible party. It confers various rights to the data subject. Firstly, it grants him or her right to access and view his or her personal information after providing an acceptable proof of identity. Under this right, the data subject is entitled to obtain information of whether the responsible party holds information about him or her in his or her custody or not and to be given a record content of that information.[984]

Secondly, it gives the data subject the right to request for correction or deletion of any personal information about him or her that is held by the responsible party. The deletion or correction is justified only when the data is inaccurate, irrelevant, excessive, out of date, misleading or that is obtained unlawfully.[985]The same right allows him to request the responsible party to delete or destroy any record of his or

[980] Ibid, section 20 (b).
[981] Ibid, section 22 (2).
[982] Ibid section 22(1).
[983]Wong, R., Data Security Breaches and Privacy in Europe. (E-book) Springer London, 2013. Accessed from https://www.rd.springer.com/book/10.1007%2F978-1-4471-5586-7, on 3rd February 2019.
[984] POPI, Section 23(1)(a) and (b).
[985] Ibid, section 24(1)(a).

her personal information because the latter is no longer authorised to retain it because the data are no longer required-for the purpose for which they were collected.[986]In terms of this section, the responsible party is obliged to inform the data subject if the correction requested is effected and whether the statement is attached.[987]

However, the section also gives the responsible party the right to refuse the requested deletion or correction. Conversely, he/she has to give a statement explaining that the requested deletion or correction was denied.[988]Moreover, if it is reasonably practicable, third parties to whom the information that is misleading, inaccurate, or incomplete has been disclosed to, should be informed of the steps taken.[989]This condition trails from the openness condition. However, unlike the openness condition, the former requires not only that the data subject be aware of his or her personal data being processed but also to be able to access and view such data.[990]

Besides the personal information conditions explained above, it is worth noting that the Act also provides for trans-border data flow. Under this heading it prohibits the responsible party from transferring personal data of a South African resident to other countries.[991] However, this prohibition is subject to several exceptions. The first exception is to the effect that personal data may be transferred if the recipient is subject

[986] Ibid, section 24(1)(b).
[987] Ibid, section 24(4).
[988] Ibid, section 24(2).
[989] Ibid, section 24(3).
[990]Abdulrauf, note 951, supra.
[991]POPI, chapter 9.

to a law, binding corporate rules,[992] or a binding agreement providing an adequate level of personal data protection.[993]

According to the law, the level of protection required should be substantially similar to the condition of the lawfully processing of personal data as provided in the POPI Act.[994] This implies that personal data may be transferred outside of South African border only if it will be subject to satisfactory data protection principles in a similar or stringent standard than South Africa's. Secondly, the prohibition is not applicable if the data subject consents to the transfer.[995] Further, it is not prohibited to transfer data to third party country if it is essential for the implementation of a contract between the data subject and the responsible party.[996]

Similarly, the prohibition does not apply when the transfer is necessary for the conclusion or implementation of a contract concluded in the interest of the data subject between the responsible party and the third party.[997] Similarly, it is not prohibited to transfer personal data to a third party country if it benefits the data subject and it is not reasonably practicable to get his or her consent and if it could have been practicable possible, he or she would have given it.[998]Most importantly, these provisions are necessary to comply with the GDPR, which prohibits member states from transferring

[992]Section 72(2) defines binding corporate rules as personal information processing policies, within group undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.
[993] Section 72(1)(a).
[994] Ibid, section 72(1)(a)(i).
[995] Ibid, section 72(1)(b).
[996] Ibid, section 72(1)(c).
[997] Ibid, section 72(1)(d).
[998] Ibid, section 72(1)(e).

personal data to third countries which does not provide adequate level of data protection.[999]

Apart from the privacy protection principles, the Act also provides for the conditions for the processing of special categories of personal data. It prohibits the processing of this kind of information unless general and specific exemptions are applied. It provides for four categories of this kind of information. The first category listed is sensitive personal information, which includes any information concerning person's religious or philosophical beliefs, race, or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour.[1000]

The second category provided is relating processing of personal information of children. The Act prohibits the responsible party from processing such information unless authorised by the Act.[1001]However, these prohibitions are to the effect that if the exemptions are provided for, the special personal information can be processed subject to the other conditions of data processing already discussed above. It is noteworthy that the prohibition imposed on processing these categories of information is subject to general exemptions applicable to all special personal information and specific exemptions applicable to particular types of sensitive information only. It is important to highlight that the GDPR does not provide for special provision regulating

[999] Article 45 of the GDPR.
[1000] POPI Act, Section 26.
[1001] Ibid, section 34.

the processing personal information relating to children. This implies that the POPI Act provides stronger protection to vulnerable class of individuals than GDPR.[1002]

Furthermore, direct marketing is the third category of processing personal data in specific context provided in the Act. Generally, the Act prohibits processing of data subject's personal information for direct marketing.[1003] The prohibition entails but not limited to any form of electronic communication such as automatic calling machine, facsimile machine, SMSs and email.[1004]However, there are exceptions to this provision. These are to the effect that processing of personal information for direct marketing can be carried out if the party responsible has consented the processing or if he or she is a customer of the responsible party.[1005]

Moreover, the fourth category provided for special processing context is fully automated decision making.[1006]The Act prohibits profiling of individuals for the intention of making automated decisions about them relying on those profiles.[1007]The Act provides that the data subject may not be subject to a decision which results in legal consequences for him, her, or it, or which affects him or her to substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance of work,

[1002]Makulilo, note 935, supra.
[1003] POPI Act, section 69 (1).
[1004] Ibid.
[1005] Ibid, section 69(1)(a) - (b).
[1006] Automated decision making occurs where information which relates to the individual is structured in such a way that it can begin to answer questions about that person, so as to put his or her private behavior under surveillance. South African Law Reform Commission (SALRC) (2009), Privacy and Data Protection Report. Para 5.2.1. Accessed from http://www.justice.gov.za/salrc/dpaper/dp/109.pdf, on 5th February 2019.
[1007] Ross, note 975, supra.

or his or her credit worthiness, reliability, location, health, personal preferences or conduct.[1008]This implies that the Act prohibits the act of subjecting the data subject to an automated decision that has its basis from their own personality profile.

However, automated decision making is allowed by the law if it is for the intention of concluding a contract and the request of the data subject in the terms of the contract has been met and if proper measures have been taken to protect the data subject's lawful interests.[1009] In addition, it is also allowed if the decision is governed by a code of conduct in which appropriate measures are laid down for protecting the lawful interest of data subjects.[1010] This is in line with Article 21 and 22 of the GDPR that provide for the automated individual decision-making including profiling.

6.4 Conclusion

The presented scrutiny and examination of security and privacy issues in South Africa reveals that privacy concerns are relatively higher than in other African countries. There are a number of reasons which justify the concerns. First, the fresh memories of the trauma caused by the past injustice of the apartheid regime are argued to be among the main catalysts influencing these concerns. It is also maintained that due to this background, privacy has been protected through the common law of delict since a long time. This is supported by the decision of O'Keeffe, the first landmark case of privacy, decided in 1954.

Secondly, the recognition of privacy right in the Interim Constitution of South Africa

[1008] POPI Act, section 71(1).
[1009] Ibid, section 71(2)(a).
[1010] Ibid, section 71(2)(b).

in 1994 became the driving force of the acceptance of this right. The right gained its current status in 1996 when it was incorporated in the Constitution of the land. Thirdly, the adoption of IT technology (cloud computing inclusive) is higher in South Africa than in other parts of Africa and hence higher concerns of privacy. Thirdly, the pressure from EU through the repealed Directive 95/46/EC, articles 25 and 26, which called non-EU member states to adopt data protection legislation that would attain the EU adequacy standard. Due to the fact that South Africa engages in many commercial activities with the EU, it felt the compulsion to adopt data and privacy protection Act of 2013. Currently, it is in the verge of enforcing an omnibus privacy protection Act.

Besides, regardless of the fact that privacy is protected through general laws as well as through statutes, there is inadequacy of law in protecting privacy and security in the cloud. Indeed, privacy and security are to some extent, protected through other laws as well as through the constitution and the common law. Nonetheless, those laws are faced with some limitations. First, they are sector specific and hence protect privacy in that sector only. Secondly, and most importantly, they are not technological neutral[1011] and hence not applicable to cloud technology. These limitations are likely to hinder South Africa's desire of protecting privacy and security in the cloud. Likewise, while POPI Act is a specific law regulating the privacy, it has not entered into force except for some of its sections for the establishment of the office of the regulator.

[1011]The term technologial neutral defines the scope of the regulation. It means that the same principles of regulation should apply despite the type of technology used. This means that the same principles of regulation should be applied whether in automated or non untomated means of communication, or whether in cloud computing or traditional computing technology. See Maxwel, W., and Bourreau, M., Technology Neutrality in Internet, Telcoms and Data Protection Regulation. Accessed from http://www.papers.ssrn.com, on 20th September, 2019.

CHAPTER SEVEN

COMPERATIVE CONCLUSIONS AND RECOMMENDATIONS

7.1 Introduction

This chapter sums up the main insights and key findings of the study and provides conclusion of the study. It also provides the recommendations and suggests niches for future research agenda.

7.2 Key Findings and Main Insights of the Study

The present study was done through a systematic investigation and analysis of the legal challenges involved in the use of cloud computing. With regard to this, the study established that until recently African states were not in the forefront data security and privacy in data protection field. However slowly the trend is changing and today Africa is striving to enact or adopt privacy and data protection regulations, both at regional and sub-regional level. The review revealed that currently 25 African countries have data protection legislations and 7 have data protection bills in place. It was noted that international instruments under the auspices of UN provided a normative basis of privacy protection in many countries regardless of the fact that UN guidelines were not legally binding. These instruments include the UDHR, ICCPR and UN guidelines.

The study also found that international agreements influence security, privacy and data protection regulations in Africa. Examples are agreements under the auspices of the OECD such as Council of Europe, European Union, the OECD guidelines, Council of Europe Convention 108, and Directive 95/46/EC, which is recently repealed by the GDPR. In addition, GDPR and its predecessor (the EU 1995 Directive) were found to

be the catalyst for the growth of the current data protection regime in Africa.

Overall, the study found a number of flaws in privacy and security in the cloud despite the shown efforts. Using Tanzania and South Africa, the study examined the appropriateness, adequacy, and relevancy of the existing legal framework in regulating privacy and security issues in the cloud in Tanzania and South Africa. It also analysed the relevance and adequacy of the international benchmarks in regulating and protecting privacy and security in the cloud in the selected countries. To achieve the intended overall objectives, three specific research questions guided the study: -

(i) what are the legal challenges emanating from the use of cloud computing?

(ii) how do the existing legal and regulatory framework and the practices protect privacy and security in the cloud in Tanzania and South Africa?

(iii) to what extent are the general principles and guidelines of the best practices relevant in protecting privacy and security in the Cloud Tanzania and South Africa?

In examining these research questions, the traditional doctrinal research methodology was used. It was supplemented by historical and comparative legal research methods. Tanzania and South Africa were used as case studies. Meanwhile, international benchmarks regarded as best practices as well as regional model laws were also included in the analysis. The study, particularly in the literature review, disclosed that there is a dearth of literature on cloud computing as well as security and privacy of data in African perspective.

Accordingly, the conceptual and theoretical analysis as well as discussion of cloud

computing, privacy and security made in chapter two, three and four, exposed that the adoption of cloud computing has given rise to a number of legal challenges relating to security and data privacy. First, the study found that while the protection of privacy is provided in Tanzanian constitution, the constitution is very narrow in scope such that it does not accommodate protection of security and privacy in the cloud. Likewise, the study established that the then existing laws and regulations besides the constitution, were not technological neutral and hence, did not encompass technologies such as cloud computing.

Tanzania sectoral laws, for example have some elements of privacy protection. Examples of these include EPOCA, Human DNA Regulation Act, Identification of Persons Act, Cyber Crime Act, Tanzania Intelligence and Security Act, HIV and AIDS (Prevention and Control) Act, to mention just a few. However, privacy protection accorded by these sectoral laws in Tanzania was found to be very limited in scope. The laws in health sector, security sector and the communication sector, for instance, protected privacy in an ad hock style: and only in those specific sectors. Similarly, most of the laws were not technological neutral and hence could not provide for cloud computing.

Likewise, the study establishes that South African Constitution also provide for the right of privacy. However, the right provided therein is too broad in interpretation, which limited its applicability. The study found that the court had from time to time to intervene and interpret its applicability to suit the issue as hand, which is a stern challenge in protection of security and privacy in the cloud. Further, it was established that South Africa has also sectoral laws with some elements of privacy protection.

These includes laws such as CPA, NCA, National Health Act, Children's Act, the Choice of Termination of Pregnancy Act, PAIA, ECA, ECTA and RICA.

Nonetheless, most of the laws were not technological neutral and hence did not apply to cloud computing privacy and security. Equally, the laws have no general application, they are applicable to the specific sectors only. Indeed, South Africa had omnibus data privacy protection law, known as POPI Act, geared toward privacy and security holistically. Nonetheless, it had not entered into force since its adoption: except some few sections that established the office of the regulator. Moreover, POPI was not in line with technology, and thus could not protect security and privacy in the cloud even if it were to come into force.

The findings generally implied that the then existing laws in Tanzania and South Africa respectively did not holistically protect privacy right. In other words, security and privacy of data in the cloud was inadequately protected by the existing legal frameworks and legislation regardless of the initiatives and campaigns of cloud adoption in the countries. The second legal challenge found was the lack of integration between technology and regulation in protection of security and privacy in general and in the cloud. It was revealed that although legislation and regulation are effective techniques for protecting security and privacy, they are not enough.

In order to have a proper protection of security and privacy in the cloud, there should be an integration of regulation and technology. The regulation side should entail laws and regulations, likewise, technology aspect should include designing for privacy or coding for privacy. This involves the use of technical and administrative actions in the

information systems to deter invasion of security and privacy of personal data in the cloud.

In addition, the analysis and discussion of the general principles and guidance of the best practice and its relevance to Tanzania and South Africa in protecting privacy and security in the cloud in chapter four, five and six revealed the that: General principles of data protection included lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation principle, security and confidentiality principle and accountability principle. These principles were found to be very relevant to Tanzania and South Africa in protecting security and privacy protection in the cloud. This was justified by the fact that the same principles had been incorporated in the draft bill of data protection in Tanzania as well as in POPI Act in South Africa.

However, the fact that the draft bill had not been made into law derogated the relevancy of these principles in Tanzania. The same applied to South Africa, as the POPI Act had not yet come into force. Similarly, the relevancy of these principles was depicted from the fact that the same principles were, to some extent, in an ad hock style, incorporated in the sectoral laws for privacy protection in both countries. However, their relevancy and applicability were limited to specific sectors alone and thus did not protect privacy holistically. That being said, it is clearly established that as of the time of study, the principles had limited relevancy to Tanzania and South Africa, as they were not in operation to protect security and privacy in the cloud.

7.3 Recommendations

Cloud computing is currently the technology that is revolutionising our world. However, to be able to tap all its potentials, among other things, there is the dire need to have proper legal and regulatory framework that regulates privacy and security in the cloud. Consequently, the thesis recommends the following measures in addressing privacy and security issues in the cloud:

First, Tanzania should enact data protection regulation which will regulate the processing personal data and hence protect privacy right. The law should be technologically neutral so that it can encompass cloud computing and other technological developments. The proposed robust omnibus data protection regulation should reflect all universally accepted data protection principles as promulgated in the best practices. This is imperative in this era of the GDPR so that the law can meet the adequacy standards as provided in GDPR. Being in line with the adequacy standard enables the country to transfer personal information to other jurisdictions and hence facilitating trade and other relations.

Secondly, Tanzania should amend or substantially overhaul the draft bill before it is passed into law. This is because the draft bill, as it stands, has many flaws that if it is passed into law as it is, can water down its effectiveness in protection of privacy. For instance, the bill has not provided for the administrative conditions to be adhered to before processing personal data. This includes the need of giving notice to the data commissioner before processing personal data. Further, the bill does not provide for the requirement of obtaining data subjects' consent before data collection. Considering, that the consent is essential factor in assessing the legality of data

processing in international instruments and the draft bill needs to accommodate it. Its omission, suggests that the law that will follow will be incompetent.

Thirdly, together with the initiatives of protecting security and privacy in the cloud through legislation and regulation, there is the need for integrating technological and legislative means of data protection in Tanzania and South Africa respectively. This is because regulations and legislation alone are not enough in protecting security and privacy in the digital age (albeit in the cloud). This is supported by the concept that legislation evolves as a function of years while technology develops as a function of weeks and months. Therefore, to keep abreast with changes in technology, law and technology need to be integrated. This is known as privacy by design and default or privacy by code. This implies that computer scientist and engineers are to be trained to design and develop information and communication systems that will minimize access to data and hence control processing of personal data in the cloud.

Fourthly, it is recommended that Tanzania should learn and emulate South Africa in relation to preparation of the data protection legislation. It goes that there is the need for Tanzanian policy makers to comprehend that preparation of data privacy legislation is not a task that should be done in a rush. This does not mean that the task should take excessively long time such as POPI Act of South Africa. Besides, the task calls for vigilant deliberations of law, which is necessitated by the complexity of different matters intricate in the making of data privacy laws. This implies that it should not simply be a task of 'cut' and 'paste' of an alien data privacy law. It is also imperative that institutions such as the Law Reform Commission of Tanzania (LRCT) should be given the task of preparing data privacy law. The above recommendation

has its basis in South Africa, where the SALRC was given the task of preparing the POPI Act and it did a good job. This implies that this noble task should be assigned to a special task force established for that purpose only.

Fifth, the LRCT should work together with a team of specialists in privacy laws. These may include renowned experts of data privacy laws. This is because it is a specialised area, which requires in-depth research in drafting the legislation. Furthermore, the committee should learn from the SALRC team for privacy to devote adequate period of time. Adequate time should be set aside for analysing and evaluating privacy legislations from other countries to tap meaningful lessons to be applicable in their home countries. This is justified by the necessity of comparative study as discussed in Chapter One of this work.

Sixth, it is recommended that the proposed data privacy law be in line with international data privacy legislations. This implies that the latter should be a basis for vigorous interaction with the international data privacy rules, to reflect the new developments in the international sphere. A lesson can be learnt from South Africa where POPI Act obliges the Regulator to constantly monitoring new developments in the international sphere. In addition, Section 40 and 44 of the Act assigns an ambassador role to the Regulator, to interact with other regulators in the world. Tanzania should emulate the South African approach by incorporating in the proposed law provisions, which will oblige the Regulator to interact with other regulators/DPAs and monitor the development in data privacy spheres at the international level.

Seventh, it is recommended for South Africa that POPI Act should be amended or overhaul substantially before it enters into force so that it can accommodate changes

and development in technology. This is because it was enacted after the EU Directive of 1995, which is now repealed by the GDPR for the want of among other things to be in abreast with technology. Likewise, it is recommended that POPI Act should enter into force as soon as it is practicable. This is because enacting an omnibus data protection regulation is not enough without enforcing it. That is POPI Act will only protect privacy and security in the cloud when it enters into force.

7.4 Future Research Agenda

The present study has provided general analysis of privacy and security issues in the cloud in Tanzania and South Africa only. The findings are slightly similar with some idiosyncrasies for individual countries. The differences suggest that the findings cannot be applied to other African nations with unlike conditions. This necessitates the need to conduct similar research in other African countries. In addition, it is necessary to assess the adequacy of emerging legislation in different states in Africa in protecting privacy and security in the cloud. Lastly but not least, the coming into force of the GDPR in May, 2018, calls for further research to assess how the emerging privacy regimes in Africa align with the adequacy standard provided therein.

BIBLIOGRAPHY

451 Research LLC and Its Affiliates (2015) Data Privacy in the Cloud Report, New York, London, San Francisco, Boston, May 2015.

Abdulaziz, A. (2012). Cloud Computing for Increased Business Value. *International Journal of Business and Social Science*, *3*(1).

Abdulrauf, L. A. (2016). *Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (LLD dissertation). University of Pretoria, Pretoria.

Access now Team. (2014). African Union Adopts Framework on Cyber Security and Data Protection.

Adrian, A. (2013). How Much Privacy do Clouds Provide? An Australian Perspective. *Computer Law and Security Review*, *29*(1).

African Union. (2014). List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.

Ahmed, M., & Hossain, M. A. (2014). Cloud Computing and security Issues in the Cloud. *International Journal of Network Securities & Its Applications (IJNSA)*, *6*(1).

Alfino, M., & Mayes, G. R. (2003). Reconstructing the Right to Privacy. Social Theory and Practice, 29(1), 1-18.

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, New Jersey: Rowman & Littlefield.

Allmer, T. A. (2011). A Critical Contribution to Theoretical Foundations of Privacy Studies. *Journal of Information, Communication and Ethics in Society*, *9*(2).

Allouche, G. (2014). How Safe is your Cloud Data from Service Traffic Hijacking?

American Institute of Certified Public Accountants (AICPA) and CICA. (2009). Generally Accepted Privacy Principles.

AN, Y. Z. (2016). Reviews on Security Issues and Challenges in Cloud Computing. A paper presented in IOP Conference Series: Materials Science and Engineering 160.

APEC. (2011). APEC at Glance.

Ardent, H. (1958). *The Human Condition*. Chicago: University of Chicago Press.

Arutynov, V. V. (2012). Cloud Computing: Its History of Development, Modern State and Future Considerations. *Scientific and Technical Information Processing Journal*, *39*(3).

Attaran, M. (2017). Cloud Computing Technology: Leveraging the Power of Internet to Improve Business Performance. *Journal of International Technology and Information Management, 26*(1).

Australian Human Rights Commission. (2018). What is the Universal Declaration of Human Rights?

Avizienis, A., Laprie, J., Brian, R., and Landwehr, C. (2004). Basic Concepts and Taxonomy of dependable and Secure Computing. *IEEE Transactions and Dependable and Secure Computing Journal,1*(1).

Barbara, J. J. (2009). Cloud Computing: Another Digital Forensic Challenge.

Beardsley, E. (1971). *Privacy: Autonomy and Selective Disclosure*, (J. R. Pennock, & J. W. Chapman, Eds.), Nomos XIII. Atherton Press: New York.

Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and United States*. Cornell University Press, Ithaca/London.

Berkman, B. A. (1971). The Assault on Privacy: Computers, Data Banks, and Dossiers by Arthur R. Miller22 Case W. Res. L. Rev.808.

Bhawan, L. N. (2013). Legal and Policy Issues in Cloud Computing, a discussion Paper based on DSCI-BSA Workshop, Data Security Council of India.

Bhowmik, S. (2017). *Cloud Computing*. Cambridge University Press: London.

Bing, J. (1984). The Council of Europe Convention of the OECD Guidelines on Data Protection. *Michigan Journal of International Law*, *5*(1).

Birnhack, M. D. (2008). The EU Data Protection Directive: An Engine of a Global Regime. *Computer Law & Security Review*, *24*(6).

Blume, P. E. (2010). *Data Protection and Privacy – Basic Concepts in Changing World*, (P. Blume, ed). Scandinavian Studies in Law Volume 56, ICT Legal Issues, Jure Law Books, Stockholm.

Bobonich. C. (2011). *Plato's Laws: a critical Guide*. Cambridge University Press: MA.

Bohm, M., Leimeister, S., Riedl, C., and Krcmar, H. (2011). Cloud Computing and Computer Evolution, Cloud Computing Technologies, Business Models, Opportunities and Challenges, TechnischeUniversitatMunchen (TUM) Germany, Journal.

Boshe, P. (2016). *Data Privacy Law Reforms in Tanzania* (A.B. Makulilo, ed) African Data Privacy Laws, Springer, International Publishing AG, Switzerland.

Bratman, B. E. (2002). Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy. *Tennessee Law Review*, Vol 69.

Burchel, J. (2009). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law*, *13*(1).

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, Hype, and Reality for Delivering Computing as the 5th utility. *Future Generation Computer Systems, 25*(6).

Bygrave L. A. (2010). Privacy and Data Protection in an International Perspective; Scandinavian Studies in Law, Vol 56.

Bygrave, L. A. (2014). *Data Privacy Law- An International Perspective* (1st ed.). London: Oxford University Press.

Bygrave, L. A. (1998). Data Protection Pursuant to the Right in Human Rights Treaties. *International Journal of Law and Information Technology*, *6*(3).

Bygrave, L. A. (2000). European Data: Determining Applicable Law pursuant to European Data Protection Legislation. *Computer Law & Security Report,16*(4).

Bygrave, L. A. (2008). *International Agreements to Protect Personal Data*, (J. B. Rule, & G. Greenleaf, eds). Global Privacy Protection, The First Generation. Cheltenham, UK/ Northampton, MA, USA: Edward Elgar Publishing Limited.

Bygrave, L. A. (2008). Privacy Protection in a Global Context- A Comparative Overview.

Bygrave, L. A. (2001). The Place of Privacy in Data Protection Law. *University of Wales Law Journal, 24*(1).

Byrne, E. F. (1998). *Privacy* (R. Chadwick, ed) encyclopaedia of Applied Ethics, Vol.3. San Diego, CA: Academic Press

Caithness, N., Drescher, M., and Wallom, D. (2017). Can Functional Characteristics Useful Define the Cloud Computing Landscape and is the Current Reference

Model Correct? *Journal of Cloud Computing: Advances, Systems and Applications*.

Canadian Institute of Health Research (CIHR). (2011). Selected International Legal Norms on the Protection of Personal Information in Health Research.

Casagran, C. B. (2017). *Global Data Protection in the Field of Law Enforcement: An EU Perspective*. Routledge: New York.

Cate, F. H., Cullen, P., and Mayor-Schonberger, V. (2013). *Data Protection Principles for the 21st Century*, Books by Maurer Faculty 23: Redmond WA.

Catteddu, D., & Hogben, G. (2009). *Cloud computing Benefits, Risks and Recommendations for Information Security*. In Serrao, C., Aquilera Diaz, V., Cerullo, F., (eds) Web Application Security. IBWAS. Communications in Computer and Information Science, Vol 72. Springe: Berlin, Heidelberg.

Chang, H. (2015). Data Protection Regulation and Cloud computing, (Cheung, A. S. Y. &Weber, R. H., eds) Privacy and Legal Issues in Cloud Computing. Edward Elgar Publishing Limited: Cheltenham.

Chassang, G. (2017). The Impact of EU General Data Protection Regulation on Scientific Research. *Ecancer Medical Science Journal,11*(709).

Chavan, P., & Kulkarni, G. (2013). PaaS Cloud. *International Journal of Computer Science and Information Security (IJCSIS, 1*(1).

Cheung, A. S., & Weber, R. H. (2015). *Privacy and Legal Issues in Cloud Computing*. Cheltenham, England: Edward Elgar Publishing Limited.

Chiueh, S. N., & Brook, J. (2015). RPE Report.

Ciochon, R. C. (2015). *Privacy and Personality* (1st ed.), New York: Routledge.

Citron, D. K., & Henry, L. M. (2010). Visionary Pragmatism and the Value of Privacy

in the Twenty-one Century. *Michigan Law Review*, *108*.

Cloud Security Alliance. (2011). Security guidance for Critical Areas of Focus in Cloud Computing.

Council of Europe. (2018). Chart of Signatures and Ratifications of Treaty 108.

Council of Europe. (2018). Details of the Treaty No. 108.

Cousens, A., & Heyder, M. (2015). *Apec Privacy Rules for Cross-Border Data Flows-A Model for Global Privacy Protections*.

Crook, J. R. (2004). Cousens, A., & Heyder, M. (2015). Apec Privacy Rules for Cross-Border Data Flows-A Model for Global Privacy Protections. *North-Western University Journal of International Human Rights,1*.

Crowe, D. (2017). Cloud Adoption in South Africa.

Davis, F. (1959). What do we mean by "Right to Privacy"? *San Diego Law Review*, *4*.

Davis, S. (2009). Is there a right to Privacy? *Pacific Philosophical Quarterly*, *9*(4).

De Filippi, P., & Belli, L. (2012). Law of the Cloud V Law of the Land: Challenges and Opportunities for Innovation. *European Journal for the Law and Technology*, *3*(2).

De Hert, P., & Papakonstantinou, V. (2012). The Proposed Data Protection Regulation Replacing Directive 95/46/EC: a sound system for the protection of Individuals. *Computer Law & Security Review*, *28*(2).

De Cew, J. W. (1997). *In Pursuit of Privacy: Law Ethics and Rise of Technology*. Ithaca, New York: Cornell University Press.

DeCew, J. W. (2018). the Stanford encyclopaedia of Philosophy. In *the Stanford encyclopaedia of Philosophy*, (Spring Edition, Vol. 1).

Deloitte. (2017). Privacy is Paramount: Personal Data Protection in Africa.

Diggelmann, O., & Cleism, N. V. (2014). How the Right of Privacy Became a Human Right? *Human Right Law Review*, *14*.

DLA Piper. (2017). Data Protection Laws of the World, South Africa.

Dobinson, I., & Johns, F. (2007). *Qualitative Legal Research' in McConville, M., and Wing, H. C., (eds) Research Methods for Law*. Edinburgh: Edinburgh University Press.

Eberle, E. J. (2009). The Method and Role of Comparative Law. *Washington University Global Studies Law Review*, *8*(3).

Elder, T., Yarrison, F. W., & Long, B. L. (2015). An Empirical Investigation of Privacy: The Impact of the Multiple Levels of Trust, A paper prepared for the American Sociological Association Annual meeting at Kent State University.

Elgesem, D. (1999). The Structure of the rights in Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data. *Ethics and Information Technology Journal*, *1*(4).

Emma, L. (2018). Importance of Technology in the workplace.

Erl, T., Mahmood, Z., & Puttin, R. (2013). *Cloud Computing; Concepts, Technology & Architecture*. New York: Service Tech Press.

Esselaar, S., & Adam, L. (2013). *Understanding what is happening in Tanzania: Evidence of ICT Policy Action,* (2nd ed., Vol. 1). Dar Es Salaam.

European Data Protection Supervisor. (2018). The History of the General Data Protection Regulation.

Handbook for European Data Protection Law. (2018). *Handbook for European Data Protection Law*. Luxembourg.

Farber, D. A. (1993). Book Review: Privacy, Intimacy, and Isolation by Inness, J., C., *Constitutional Commentary*, *10*(2).

Floridi, L. (2006). Four Challenges for a theory of Informational Privacy. *Ethics and Informational Technology Journal*, *8*(3).

Foye, S. (2008). Book Review on Understanding Privacy by Solove, D., J. *Journal of High Technology Law*.

Fried, C. (1984). *Privacy (a moral analysis), in Schoeman, F.D., (Ed) Philosophical Dimensions of Privacy*. New York: Cambridge University Press.

Fried, C. (1968). Privacy. *Yale Law Journal, 77*.

Fuchs, C. (2011). Towards an Alternative Concept of Privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4).

Gartner Inco. (2011). Gartner identifies the top 10 strategic technologies for 2011.

Gartner. (2016). Worldwide Public Cloud Market to Grow for 17 percent.

Gavison, R. (1980). Privacy and the Limits of the Law. *The Yale Law Journal*, *89*(3).

Gebers, J., & Ophoff, J. (2013). Exploring Cloud Computing Legal & Privacy Issues in South Africa. A Conference Paper Presented in World Wide Web Applications Conference in Cape Town, on 10th to 13th September 2013.

Geetu, G., & Sandhya, V. (2016). A Survey on Issues of Security in Cloud Computing. *International Journal of Advanced Research in Computer Science*, *7*(6).

Gerstein, R. S. (1984). *Intimacy and privacy, in Schoeman, F.D. (Ed.), Philosophical Dimensions of Privacy*. Cambridge: Cambridge University Press.

Giessmann, A., & Stanoevska, K. (2012). Platform as a Service- A Conjoint Study on Consumers" Preferences, a paper submitted in 33rd International Conference

on Information Systems, (ICIS) Orlando.

Gilliland, A. T. (2018). The General Data Protection Regulation: What does it Mean for Libraries worldwide?

Gillwald, A., Moyo, M., & Stork, C. (2012). Understanding what is happening in ICT in South Africa-a Supply- and demand -side analysis of the ICT sector.

Gillwald, A., & Moyo, M. (2013). Prospects, Challenges and Impacts of Cloud: Perspectives from (South) Africa. A Presentation to UNCTAD Workshop on Cloud Economy, Geneva, February 2013.

Gillwald, A., Moyo, M., Odufuwa, F., & Kamoun, F. F. (2013). The Cloud Over Africa.

Giuseppe, A., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. In Proceedings of the 14th ACM Conference on Computer and Communications Security.

Goel, A., & Goel, S. (2012). Security Issues in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management*, *1*(4).

Gorska, Z. M. (2008). *Privacy, Surveillance and Hiv/Aids in the Work Place: A South African Case Study*(dissertation). University of Witwatersrand, Johannesburg.

Greenleaf, G. (2004). The APEC Privacy Initiative: 'OECD Lite' for the Asia- Pacific. *Privacy Laws &Business Journal*, *71*(5).

Greenleaf, G. (2011). *Global Data Privacy Laws: Forty Years of Acceleration*. Wales, London: Privacy Laws and Business International.

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalizations of Convention 108. *International Data Privacy Law*, *2*(2).

Greenleaf, G., & Georges, M. (2015). The African Union's Data Privacy Convention: A Major Step Toward Global Consistency? *Privacy Laws & International Business Journal Report*, *131*(3).

Greenleaf, G. (2017). Global Data Privacy Laws: 120 National Data Privacy Laws, Including Indonesia and Turkey. *145 Privacy Laws & Business International Report 10, UNSWLRS*, *45*.

Greenleaf, G. W. (2014). *Asian Data Privacy Law: Trade and Human Rights Perspective*. Oxford University Press.

Griffith, E. (2016). What is Cloud Computing?

Gutwirth, S. (2002). *Privacy and Information Age*. Rowman & Littlefield Publishers Inc.

Hashzume, K., Rosado, D., Fernandez-Medina, E., & Fernandez, B. E. (2013). An analysis of Security Issues for cloud Computing. *Journal of Internet Services and Applications*, *4*(5).

Heeney, C., & Weigand, H. (2013). Privacy Protection and Communicative Respect, Proceedings of the 8th International Working conference on the Language-Action Perspective on Communication Modelling (LAP), Tilburg, the Netherlands.

Herbst, N. R., Kounev, S., Reussner, R., & Nikolas, E. (2013). Elasticity in Cloud Computing: What It Is and what It Is Not? Proceedings for the 10th International Conference on Autonomic Computing (ICAC, 2013), San Jose, CA, June 24-28, 2013.

Heyink, M. (2011). Protection of Personal Information for South African Law Firms. LSSA Guidelines, SALRC Report.

Heyink, M. (2018). Protection of Personal Information Guidelines for South African Law Firms.

Hilberg, R. (1985). *The Destruction of the European Jew*. Holmes & Meier Publishers.

Hill, K. (2015). Cloud Computing Emerging in Africa.

Hofer, C. N. (2011). Cloud Computing Services: Taxonomy and Comparison. *Journal of International Services Applications*, *2*(5).

Hondius, F. W. (1980). Data Law in Europe. *Stanford Journal of International Law*, *16*(5).

Hondius, F. W. (1983). A Decade of International Data Protection. *Netherlands International Law Review*, *30*(2).

Hussein, N., & Abdelbaki, N. (2013). *It legal Framework for Cloud Computing*. Springer-Verlag.

IBM. (2014). What is Cloud Computing.

Inness, J. C. (1992). *Privacy, Intimacy and Isolation.* Oxford University Press.

Iqbal, S., Kiah, L. M., Anuar, N. A., Daghighi, B., Wahab, A. W., & Khan, S. (2016). Service Delivery Models of Cloud Computing: Security Issues and Open Challenges. *Security and Communication Network Journal*, *9*(17).

Issacs, R., Crawford, K., & Fulbright, R. N. (2018). Data Protection Law in South Africa: Overview.

ITU. (2012). Cloud Computing in Africa- Situation and Perspectives.

ITU. (2012). Privacy in cloud Computing, ITU-Technology Watch Report- Geneva.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud. *Journal of Information Technology and Politics*, *5*(6).

Kaubar, C., & Mayers, S. (2013). When the Cloud Disperse: Data Confidentiality and Privacy in Cloud Computing.

Kaur, K. (2016). A Review of Cloud Computing Services Models. *International Journal of Computer Applications*, *140*(7).

Kerry, J., & Teng, K. (2010). Cloud computing: Legal and Privacy Issues. *Journal of Legal Issues and Cases in Business*, *5*(7).

King, N. J., & Raja, V. T. (2012). Protecting the Privacy and Security of Sensitive Customer Data in the Cloud. *Computer Law and Security Review*, *28*(3).

Kirby, M. (2011). The History, Achievements and Future of the 1980 OECD Guidelines on Privacy. *International Data Privacy Law*, *1*(1).

Kiunsi, H. B. (2017). *Transfer Pricing in East Africa: Tanzania and Kenya in Comparative Perspective*(dissertation). The Open University of Tanzania.

Kleynhans, S. (2012). The New Era, The Personal Cloud.

Kong, J., Fan, X., & Chow, K. P. (2015). *Introduction to Cloud Computing and Security Issues, in Cheung, A. S. Y. & Weber, R (eds) Privacy and Legal Issues in Cloud Computing*. Edward Elgar Publishing Limited, Elgar Law, Technology and Society.

Konvitz, M. R. (1966). Privacy and the Law: A Philosophical Prelude. *Law and Contemporary Problems Journal*, *31*(2).

Kumar, K. V. (2013). Software as a Service for Efficient Cloud Computing. *International Journal of Research in Engineering and Technology*, *3*(1).

Kumar, S., & Goudar, R. H. (2012). Cloud Computing- Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. *International Journal of*

Future Computer and Communication, *1*(4).

Kuner, C. (2009). An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, *25*(1).

Kwamboka, L. (2018). After the Facebook-Cambridge Analytical Scandal, can we talk about data Privacy in Africa now? Quarts Africa.

Lamba, H. S., & Singh, G. (2011). Cloud Computing-Future Framework for e-management of NGO's. *International Journal of Advancement in Technology*, *2*(3).

Laurel, D. (2010). 10 benefits of Cloud Computing, (Verio).

Lavelle, M. (2016). Why the Shift to Cloud Computing Reminds me of the Ford Model-T?

Leavitt, N. (2009). "Is Cloud Computing Really Ready for Prime Time?" *Computer*, *42*(1).

Lessig, L. (2006). *Code*. Basic Books Publisher.

Liver, A. (2011). *On Privacy*. Routledge.

Lloyd, I. J. (2017). *Information Technology Law* (8th ed.). Great Clarendon Street: Oxford University Press.

Lord, N. (2018). A Definition of Cloud Account Hijacking. Digital Guardian.

Loubser, M., Midgley, R., Jabavu, P., Linscort, J., Mukheibir, A., Niesing, L., Wessel, B. (2010). *The Law of Delict in South Africa* (3rd ed.). Oxford University Press of Southern Africa.

Lukas, A. (2016). What is Privacy? The History and definition of Privacy.

Maaref, S. (2012). ITU, Cloud Computing in Africa: Situation and Perspectives.

MacKinnon, C. (1989). *Towards a Feminist Theory of the State*. Harvard University

Press.

Makulilo, A. B. (2012). *Protection of Personal Data in Sub-Saharan Africa* (dissertation). University of Bremen.

Makulilo, A. B. (2016). *African Data Privacy Laws* (1st ed., Vol. 1). Springer International Publishing AG.

Makulilo, A. B., & Boshe, P. (2016). Consultation on the Commission's Comprehensive approach on Personal Data Protection in Tanzania, submitted on 31st August.

Malhotra, R., & Jain, P. (2013). International Journal of Computer and Technology. *How to Choose an Economic Cloud Deployment Model? 4*(8).

Masoud, B. S. (2012). *Legal Challenges of Cross-Border Insolvencies in Sub-Saharan Africa with References to Tanzania and Kenya: A Framework for Legislation and Policies*(dissertation).

Maxwel, W., & Bourreau, M. (2014). Technology Neutrality in Internet, Telcoms and Data Protection Regulation. *Computer and Telecommunication Law Review, 1*(1).

Mboizi, J. P. (2015). Internet and Data Protection: The African Cybersecurity Convention.

McQupid-Mason, D. J. (1996). *Privacy in Chaskalson, M., et al (eds) Constitutional Law of South Africa, Juta*. Kenwny.

Meetei, M. Z., & Goel, A. (2012). Security Issues in Cloud Computing, in 2012 5th International Conference on Biomedical Engineering and Informatics.

Mell, P., & Grance, T. (2009). A NIST Definition of Cloud Computing. National Institute of Standards and Technology.

Mgonzi, T., & Weeks, R. (2015). The Impact of Cloud Computing on the Transformation of Healthcare System in South Africa. A Conference Paper Presented in 2015 ITU Kaleidoscope: Trust in the Information Society.

Michalson, L. S. (2013). Data Privacy or Data Protection in South Africa.

Michalson, L. S. (2017). Information Regulator in South Africa.

Michalson, L. S. (2018). Guide to ECT Act in South Africa.

Moerel, L. (2011). The Long Arm of the EU Data Protection Law: Does the Data Protection Directive. Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? *International Data Privacy Law*, *1*(1).

Moor, J. H. (1991). The Ethics of Privacy Protection, Library trends. *Intellectual Freedom*, *39*(1).

Moore, A. (2008). Defining Privacy. *Social Philos*, *39*(3).

Moore, A. (2000). Employee Monitoring & Computer Technology: Evaluative Surveillance versus Privacy. *Business Ethics Quarterly*, *8*(4).

Mukami, S. (2017). Technology: We Need to Embrace Cloud Computing.

Muyinga, M. (2013). Privacy and Legal Issues in Cloud Computing. The SMME Position in South Africa. A Conference Paper presented in the 11th Australian Information Security Management Conference, Edith Cowen University Perth, Western Australia on 2nd to 4th December 2013.

Mvelase, P. S., Dlamini, I. Z., Sithole, H. M., & Dlodlo, N. (2013). Towards a Government Public Cloud Model: The Case of South Africa. A Conference Paper presented in the Second International Conference on "Cluster Computing "in L'viv, Ukraine on 3rd to 5th June 2013.

Myers, J. (2016). Which are Africa's Fastest Growing Economies?

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal. Information Act 4 of 2013 in Light of Recent International Developments, (Part 1). *THRHR Journal*, *51*(68).

Mzekandaba, S. (2014). Security Concerns Hold Back South Africa Cloud Adoption.

Naude, A. (2014). *Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Development. Ll.M. Mini Dissertation*(dissertation). University of Pretoria.

Nazir, M. (2012). Cloud Computing: Overview & Current Research Challenges. *Journal of Computer Engineering*, *8*(1).

Neethling, J., Potgieter, J. M., & Visser, P. J. (2005). *Neethling's Law of Personality*. LexisNexis.

Neethling, J., Potgieter, J. M., & Visser, P. J. (2010). *Law of Delict* (6th ed.). LexisNexis.

Neethling, J. (2012). Features of the Protection of Personal information Bill, 2009 and the Law of Delict. *Journal of Contemporary Roman-Dutch Law*, *75*(5).

Neethling, J., Potgieter, J., & Knobel, J. C. (2015). *Law of Delict* (7th ed.). LexisNexis.

New World Encyclopaedia contributors. (2017). New World Encyclopaedia. In *New World Encyclopaedia*.

New Zealand 's Law Commission. (2008). Concepts and Issues, Review of the Law of Privacy Stage 1, Study Paper.

Njue, D. (2013). Cloud Services Opportunities and Challenges for East Africa.

O'Donoghue, C. (2015). Njue, D. (2013). Cloud Services Opportunities and Challenges for East Africa. *Data and Cyber Security Journal*, *1*(1).

O'Donnell, M. K. (2009). New Dirty War Judgements in Argentina: National Courts

and Domestic Prosecutions of International Human Rights Violations. *New York University Law Review*, *84*(5).

OECD. (2001). *Oecd Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data*. Paris, France: OECD Publication Service.

Olga, E. Y. (1991). Trans-border Data Flows and the Sources of Public International Law. *North Carolina Journal of International Law and Commercial Regulation*, *6*(2).

Omwansa, T. K., Waema, T. M., & Omwenga, B. (2014). Cloud computing in Kenya, A 2013 Baseline Survey.

Orji, U. J. (2017). Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act. *International Data Privacy Law*,*1*(3).

Pal, D., Chakraborty, S., & Nag, A. (2015). Cloud computing: A Paradigm Shift in IT Infrastructure. *CSI Journal of Computing*, *38*(10).

Parent, W. A. (1983). Privacy, Morality and the Law. *Philosophy and Public Affairs*, *12*(4).

Pearson, S., & Yee, G. (2013). *Privacy and Security for Cloud Computing*. London: Springer International Publishing, Springer- Verlag .

Peikoff, A. L. (2008). Beyond Reductionism: Reconsidering the right to Privacy. *N. Y. U. Journal of Law & Liberty*, *3*(1).

Pillay, L. (2014). South Africa: Data Protection Legislation. Retrieved from Hogan Lovells Global Media and Communications Quarterly.

Posner, R. A. (1978). The right of Privacy. *Georgia Law Review*, *12*(3).

Post, R. C. (2001). Three Concepts of Privacy. *Yale Law School, Faculty Scholarship*

Series, *185*.

Privacy International & Tanzania Human Right Defenders Coalition. (2015). *The Right to Privacy in the United Republic of Tanzania, Stakeholders Report*. Universal Review.

Prosser, W. (1960). Privacy. *California Law Review*, *48*(3).

Qi, H., Shirazi, M., Gani, A., Whaiduzzaman,, M. D., & Khan, S. (2014). Sierpinski Triangle Based Data Centre Architecture in Cloud Computing. *The Journal of Super-Computing*, *69*(2).

Rajaretnam, T. (2014). The Implications of Cloud Computing for Information Privacy: An Australian Perspective. *International Journal of Business, Economics and Law*, *5*(4).

Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The Management of security in Cloud Computing. A paper presented in Information Security for South African Conference in Johannesburg.

Rani, D., & Ranjan, R. K. (2014). A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(6).

Rao, C., Leelarani, M., & Kumar, Y. R. (2013). Cloud: Computing Services and Deployment Models. *International Journal of Engineering and Computer Science*, *2*(12).

Rasool, Y. (2017). *An Examination of how the Protection of Personal Information Act 4 of 2013 (Popi) will Impact on Direct Marketing and the Current Legislative Framework in South Africa*(dissertation). University of Kwazulu- Natal.

Razaque, A., & Rizvi, S. S. (2017). Privacy Preserving Model: A New Scheme for

auditing Cloud Stakeholders. *Journal of Cloud Computing: Advances, Systems and Applications*, *6*(7).

Reeta, S. A., Rao, K. D., & Prasad, B. D. (2013). Implications of Cloud computing for Personal Data Protection and Privacy in the Era of the Cloud: An Indian Perspective. *Law Journal of the Higher School of Economics, Annual Review*, *1*(5).

Richardson, H. (2018). Characteristics of a Comparative Research Design.

Robert, M. (2016). Infrastructure as a Service, Options in Cloud Computing.

Robinson, N., Valeri, L., Cave, J., Starke, T., Graux, H., Creese, S., & Hopkins, P. P. (2010). *The Cloud: Understanding the Security, Privacy and Trust Challenges A report prepared for Unit F. 5, Director General Information Society and Media*. European Commission.

Rodero, L., Gonzalez, L., Caron, E., Murasen, A., & Desprez, F. (2011). *Building safe PaaS Clouds: A Survey on Security in Multi-Tenant Software Platforms*. INRIA.

Roos, A., & Dana, M. (2016). Data Protection. In *Information and Communication Technology Law*. Durban: LexisNexis.

Ross, A. (2008). Personal Data Protection in New Zealand: Lessons for South Africa. *Potchefstroom Electronic Law Journal*, *11*(4).

Ross, A. (2013). *The Law of Data (Privacy)Protection: A Comparative and Theoretical study*(dissertation). UNISA.

Ross, A. (2016). *Data Protection Law in South Africa, in Makulilo, A. B. (ed) African Data Privacy Laws* (1st ed.). Springer International Publishing AG.

Ross, A. (2016). *Data Privacy Law, in Van der Merwe, D., et al, Information and*

Communications Technology Law. Durban: LexisNexis.

Rouse, M. (2016). Platform as a Service (PaaS).

Rule, J. B., & Greenleaf, G. (17AD). *Global Privacy Protection* (1st ed.). Cheltenham: The first-generation Elgar Publishing Limited.

Sahandi, R., Alkhalil, A., & Opara-Martins, J. (2013). Cloud computing from SMEs Perspectives: A Survey Investigation. *Journal of Information Technology Management, 26*(1).

Salbu, S. R. (2002). The European Union Data Privacy Directive and International Relations. *Vanderbilt Journal of Transnational Law, 35*(4).

Samson, T. (2013). 9 Top Threats to Cloud Computing Security.

Saravg, A., & Kant, C. (2012). Cloud Computing Security and Privacy Concerns. *International Journal of Information Technology and Knowledge, 5*(2).

Schoeman, F. (1984). *Philosophical Dimension of Privacy: an anthology*. Cambridge: Cambridge University Press.

Sen, J. (2013). *Security and Privacy Issues in Cloud Computing, in Ruiz-Martinez, A. et al (eds) Architectures and Protocols for Secure Information Technology*. IGI- Global publishers.

Shapiro, F. R. (1985). The Most-Cited Law Review Articles. *California Law Review, 75*(3).

Shoemarker, D. W. (2010). Self-Exposure of the Self: Informational Privacy and the Presentation of Identity. *Ethics and Informational Technology, 12*(1).

Simon, M. K., & Goes, J. (2013). Assumptions, Limitations, Delimitations and Scope of the Study in Dissertations and Scholarly Research: Recipes for Success.

Singhal, A., & Malick, I. (2012). Doctrinal and Social Legal Research Methods: Merits and Demerits. *Educational Research Journal*, *2*(7).

Skolmen, D. E., & Gerber, M. (2015). Protection of Personal Information in the South African Cloud Computing Environment: A Framework for Cloud Computing Adoption, 2015. *Information Security for South African (ISSA) Johannesburg*, *2*(5), 1–10.

Sloot, B. (2014). Do Data Protection Rules Protect the Individuals and should They? An Assessment of the Proposed General Data Protection Regulation. *International Data Privacy Law*, *4*(4).

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4).

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3).

Solove, D. J. (2008). *The New Vulnerability: Data Security and Personal Information, in Chandler, A. et al., Securing Privacy in the Internet Age*. Berkeley: Stanford University Press.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.

Solove, D. J. (2011). *Nothing to Hide: The False Trade-off between Privacy and Security*. London: Yale University Press.

Solove, D. J., & Schwartz, P. M. (2018). *Information Privacy Law* (16th ed.). New York: Wolters Kluwer.

Sotto, L., Treacy, B. C., & Mclellan, M. L. (2010). *Privacy and Data Security Risks in Cloud Computing*. Electronic Commerce & Law Report.

South African Law Reform Commission (SALRC). (2009). Privacy and Data Protection Report.

Sriram, I., & Hossein, A. (2010). Research Agenda in Cloud Technologies, a paper submitted to the 1st ACM Symposium on Cloud Computing, SOCC.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in cloud Computing, Review Article. *International Journal of Distributed Sensor Networks*.

Susanto, H., Almunawar, M. N., & Kang, C. C. (2012). A Review of Cloud Computing Evolution Individual and Business Perspective. *SSRN Electronic Journal*, *4*(10).

Sweeney, M. (2012). Book Review on Understanding Privacy by Solove, D., J. *An International Journal of the Information Society*, *28*(5).

Szabo, M. D., & Kiserlet, A. (2005). Privacy. *InformációsTársadalom*, *2*(5).

Takabi, H., Joshi, J. B., & Ahn, J. (2010). Security and Privacy challenges in Cloud Computing Environments. *IEEE Security and Privacy Journal*, *8*(6).

Tan, G. J. (2008). A Comparative Study of the APEC Framework-A New Voice in the Data Protection Dialogue? *Asian Journal of Comparative Law*, *3*(1).

Tanzania- Ministry of Health and social Welfare. (2013). Tanzania National e Health Strategy 2013-2018.

Tavani, H. T. (2007). Philosophical Theories of Privacy: Implication for an Adequate Online Privacy Policy. *Metaphilosophy*, *38*(1).

Tavani, H. T. (2008). *Informational Privacy: Concepts, Theories and Controversies, in Himma, K., E., and Tavani, H., T., (eds) The Handbook of Information and Computer Ethics*. Hoboken: Wiley.

Taylor, L. (2014). *Writing a Legal Research Paper- Research Methodologies, in Scragg, J., et.al. (eds), Legal Writing: A Complete Guide for a Career in Law*.

LexisNexis.

Taylor, M., & Matteucci, M. (2010). Cloud computing. *Computer and Telecommunications Law Review*, *57*(9).

The United Republic of Tanzania, Ministry of works, Transport and Communication. (2016). National Information and Communications Technology Policy.

The White Paper -TWP. (2010). Introduction to Cloud Computing.

Thierer, A. (2008). Book Review: Solove's Understanding Privacy. *The Technology Liberation Front*, *2*(4).

Thompson, J. J. (2007). *The Right to Privacy, in Schoeman, F., D., (Ed) Philosophical Dimensions of Privacy: An Anthology*. London: Cambridge University Press.

Turahi, D. (2013). Security and Privacy: Can We Trust the Cloud? A paper presented in East African Information conference in Kampala Uganda on 13th to 14th August, 2013.

Ubena, J. (2012). Privacy: A Forgotten Right in Tanzania. *The Tanzania Lawyer*, *1*(2).

Ulyashyna, L. (2006). Does Case Law Developed by the European Court of Human Rights Pursuant to ECHR Article 8 Add anything Substantial to the Rules and Principles Found in Ordinary Data Protection Principle? A Tutorial Paper Presented at the Norwegian Centre for Computers and Law (NRCCL). Spring 2006.

Verhenneman, G., & Dumortire, J. (2013). *Legal Regulation of Health Records: A Comparative Analysis of Europe and the Us in George, C., et al, eHealth: Legal, Ethical and Governance Challenges*. London: Springer.

United Nation. (2015). The Universal Declaration of human Rights.

Van der Walt, J. C., & Midgley, J. R. (2005). *Principles of Delict* (2nd ed.).

LexisNexis.

Vanberg, A. D., & Maunick, M. (2017). Data Protection in the UK Post Brexit: The Only Certainty is Uncertainty. *International Review of Law, Computers & Technology*, *32*(1).

Vibhute, K., & Aynalem, F. (2009). Legal research Methods, Teaching Material prepared under the sponsorship of the Justice and Legal System Research Institute.

Vitkar, S. (2012). Cloud Based Model for E-Learning in Higher Education. *International Journal of Advanced Engineering Technology*, *3*(4).

Vyver, E. V., Leibowitz, C., & Smith, T. (2019). POPI: Final Regulation Published. *South Africa Financial Regulation Journal*, *1*(1).

Wacks, R. (1980). *The Protection of Privacy*. London: Sweet & Maxwell.

Wacks, R. (1993). *Personal Information: Privacy and the Law*. New York: Oxford university Press.

Wall, A. (2017). GDPR Matchup: The APEC Privacy Framework and Cross Border Privacy Rules.

Wanyama, E. (2017). What African Countries Can Learn from European Privacy Laws and Policies.

Warren, S. D., & Brandeis, L. s. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5).

Waters, N. (2008). The APEC, Asia Pacific Initiative- A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?

Weber, R. H., & Heinrich, U. I. (2012). *Anonymization*. London: Springer.

Weinstein, W. L. (2007). *The Private and the Free: A Conceptual Inquiry, in Ciochon,*

R., C., Privacy & Personality (1st ed.). New York: Routledge.

Westin, A. (1967). *Privacy and Freedom*. New York: Athenaeum.

Westin, A. (1998). Privacy in America. A historical and Socio-political Analysis. National Privacy and Public Policy Symposium, Hartford, 1995. Cited in Deighton, The right to be Let Alone. *Journal of Interactive Marketing*, *12*(2).

Whalstrom, K., & Fairweather, N. B. (2013). Privacy Theory of Communicative Action and Technology.

Whitley, E. A. (2009). *Informational Privacy, Consent and the control of Personal Data* (Vol. 14). Information Security Technical Report.

Wiesrma, W., & Jurs, S. G. (2008). *Research Methods in Education: An introduction* (9th ed.). Boston: Pearson.

Wong, R. (2013). *Data Security Breaches and Privacy in Europe*. London: Springer.

Woodrow, H. (2018). *Privacy Blueprint: The Battle to Control the Design of New Technologies*. Cambridge: Harvard University Press.

Xue, C. T., & Xin, F. T. (2016). Benefits and Challenges of the Adoption of Cloud Computing in Business. *International Journal on Cloud Computing: Services and Architecture*, *6*(6).

Yousef, L. M., Butrico, M. A., & Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing.

Youssef, A. E. (2012). Exploring Cloud Computing Services and Applications. *Journal of Emerging Trends in Computing and Information Sciences*, *3*(6).