THE CHALLENGES AND THE NEED OF LEGAL FRAMEWORK FOR DATA PROTECTION IN TANZANIA: CASE STUDY OF TANZANIA NATIONAL IDENTIFICATION AUTHORITY (NIDA)

NAGAI, MELAMARI SIMON

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE MASTER OF LAW DEGREE IN INFORMATION TECHNOLOGY AND TELECOMMUNICATION (LL. M IT & T) OF THE OPEN UNIVERSITY OF TANZANIA

2013

CERTIFICATION

The Undersigned certify that he have read and hereby recommend for examination a Dissertation entitled, **The Challenges and the Need of Legal Framework for Data Protection in Tanzania: Case Study of Tanzania National Identification Authority (NIDA);** in partial fulfillment for the Award of Master of Law Degree of the Open University of Tanzania

…….

Prof. Ian. J. Lloyd

(Supervisor)

Date…….

COPYRIGHT

This Dissertation is copyright material protected under the copyright and Neighbouring Rights Act, 1999 and other International and national enactments, in that behalf, on intellectual property. It may not be reproduced by any means, in full or in part except for short extracts in fair dealings, for research or private study, without the written permission of the Directorate of postgraduate studies, on behalf of both the author and the Open University of Tanzania.

DECLARATION

I, **NAGAI, MELAMARI SIMON**, declare that this Dissertation is my own original work and that it has not been presented and will not be presented to any other University for a similar or any other degree award.

Signature …….....……

Date...…….....……..

DEDICATION

I dedicate this Research Report to my entire Family including my Father Mr. Thomas Nagai, my Mother Juliana Thefilos Metili, my lovely Fiance` Scholastica Killagane and my two lovely Sisters Emanuela and Clara for you moral support during the entire period of preparing this Dissertation Report.

ACKNOWLEGEMENT

May I first and foremost express my heartfelt gratitude to the Almighty God for giving me strength and ability to prepare this Dissertation report and bring it to this level. Thank you God.

Secondly, I would like to express special thanks to my Supervisor Professor Ian Lloyd for tireless and careful directives he provided me with, first during lectures in Arusha and at the preparation of this Dissertation. Should I say that you have added value as to how I should reason and analyse matters professionally.

Special thanks also goes to the Director General of National Identification Authority (NIDA), Mr. Dickson Maimu for giving me a permission to pursue with my Master's Program and even assisting whenever a need arise on making sure I succeed in my program. Also to my Head of Legal Directorate Ms Sabina Nyoni for covering me up during my absence while attending studies. Thank you all.

I am also indebted to the rest of the Professors who also trained me during my course not forgetting Professor Bob Clarke and the entire management of the Open University of Tanzania not forgetting Professor Elifas Bisanda, Prof. Mbogo and Dr.Kolimba for convincing and assisting me to pursue with this course to the level of graduation. My appreciation also my programme Cordinator Mr. Gervas Emmanuel who have tirelessly responded to my calls for various assistance. Also My Classmates, you have enabled me a great deal during various discussions we had on how to better improve this Research.

And lastly, my gratitude to reach all others whom in one way or another assisted me to make this Research a reality including but not limited to Professor Sifuni Mchome of the Tanzania Commission for Universities (TCU), Mr. Adam Mambi, Consolatha Resto, Hon. Calist and Mr. Alex Makulilo for their untold support. Thanks to you all.

ABSTRACT

The main objective of this Research was to analyse various Legislations, Policies and Regulations if any, and find out if there is any Lacuna in their attempt to cover issues related to Data Protection and Privacy at large and partly to issues related to National Identification systems in particular. In doing so, the Researcher chose National Identification Authority (NIDA) of Tanzania as a Case Study mainly because NIDA has brought about new system of National Identification and has conducted registration and identification of persons. Findings has shown that there are lacuna in various Legislation touching on Data and Privacy protection in Tanzania and also there is no a piece of Legislation which is enacted to exclusively deal with Data Protection and Privacy matters exclusively, only that there are scattered pieces of Legislations each attempting to provide for data and privacy protection. In the Conclusion and Recommendations, the Researcher has recommended NIDA as the Creator and Controller of the Database of the National population Register and it intends to interface with other stakeholders, some Government Institutions and other Private Institutions, the protection of that interfaced Data would be sound and promising in the presence of Data Protection Act as those provided with such information will know their role and limitations as Data Processors. And Lastly, this Research has opened doors for other Scholars to venture more and come up with new findings regarding the Data Protection Legal Framework existing in Tanzania.

LIST OF CASES

LIST OF LEGISLATIONS

A. INTERNATIONAL INSTRUMENTS

Convention on Elimination of all forms of Discrimination against Women (CEDAW)

Convention on a right of a Child

European Convention on Human Rights

European Union Directive on Data Protection [Directive 95/46/EC]

The International Covenant on Civil and Political Rights (ICCPR)

Universal Declaration of Human Rights of 1948.

B. LOCAL LEGISLATIONS

TANZANIA

The Constitution of the United Republic of Tanzania of 1977 as amended

Electronic and Postal Communications Act [Act No.3 of 2010]

Registration and Identification of Persons Act [CAP 36 R.E 2012]

Records and Archives Management Act [Act No.3 of 2002]

NIDA Establishment Instrument of 2008

UNITED KINGDOM

The Data Protection Act of 1998

ABBREVATIONS

AG	Attorney General.
CEDAW	Convention On Elimination of all forms of Discrimination Against Women
CPD	Chief Parliamentary Draftman
EAC	East African Community.
e-Government	Electronic Government.
e-Id	Electronic Identity Card.
EPOCA	Electronic and Postal Communications Act of Tanzania.
EU	European Union.
GN	Government Notice.
ICCPR	International Covenant on Civil and Political Rights.
ICT	Information Communication Technology.
ID	Identity Card.
NIDA	National Identification Authority Of Tanzania.
OECD	Organisation Of Econimic Corporation Development.
RIPA	Registration And Identification Of Persons Act Of Tanzania.
SADC	Soutern Africa Development Community.
SSCD	Secure Signature Creation Device.
UIDAI	Unique Identification Authority of India.
UID	Unique Identification Number.
UK	United Kingdom.
UN	United Nation.

TABLE OF CONTENTS

CHAPTER ONE

1.0 INTRODUCTION

This Chapter looks on the background of the Research topic and prevailing factors that trigger the researcher to conduct research on that particular topic. The chapter guides the Researcher to concentrate on the objectives and the significance of the whole study.

The Chapter commence with the background of the research problem which explains what the topic is all about so that the reader could be aware of the topic, then the statement of the problem that guided the researcher. More over the chapter has the objectives of the study, research questions, significance of the study, scope of the study, research methodology and limitation and delimitations of the study.

1.1 Background of the Problem

Tanzania as a Country, embarked through several attempts to establish the National identification system in order to create the National population register and the National Database where the vital information of all Tanzanians, Refugee and the Legal Residents can be easily and promptly obtained. The desire and motivation behind the initiatives above is two folds;

First is the impact of the interstate Intelligence committees of the East African states of Tanzania, Kenya, Uganda and Zambia way back in 1969, when met in Lusaka Zambia as one of the measures and quest to curb illegal migration activities and foster security at large within the region . By then Kenya and Zambia were already

issuing registration/identity Cards to their respective Nationals[1].

The first major initiative on the side of Tanzania on implementing the resolution of 1969 was the enactment of Registration and Identification of Persons Act in 1986[2] in order to now register and identify Citizens, Refugees and Legal residents[3] at one time present in the United Republic of Tanzania. However, this Act was never enforced until 2011 which made it one of the few legislation not to be gazzetted for longer period.

The second one is the influences of other external forces towards that will affect or has so far affected United Republic of Tanzania. The terrorist attacks, first in Dar es Salaam and Nairobi in 1998, in New York and Washington on September 11, 2001, has prompted the need to streamline vulnerable systems in the third world environment like Tanzania. In the aftermaths of these terrorist attacks, identity has taken on a new prominence in Countries around the world[4] .

The actual implementation of National identification system was never a reality in Tanzania due to budgetary constraints since 1969 until 2006 when the Government decided to conduct the feasibility study and came with a very comprehensive Feasibility Study Report which attempted to showcase on how to effectively

[1] Gotham International Ltd, (2006**), " Feasibility Study Report for National Identification and Registration of persons Program for the Government of the United Republic of Tanzania"**, Dar es Salaam, Tanzania, at P.48
[2] Cap 36, R.E 2012 of the Tanzanian Laws
[3] See S.10(1), Ibid
[4] Gotham International Ltd, (2006**), " Feasibility Study Report for National Identification and Registration of persons Program for the Government of the United Republic of Tanzania"**, Dar es Salaam, Tanzania, at P.49

introduce and implement the National identification system in Tanzania[5] . The Feasibility study then proposed the establishment of an Institution which would implement the National identification system. This was then followed by the establishment of the National Identification Authority (NIDA)[6] in the year 2008 which finally took the role of the implementing the registration and identification of persons Act to date.

In nutshell, immediately after its establishment, NIDA has taken untold initiatives to establish the infrastructure for the implementation of National ID system which amongst others, includes creating National population Register, creating various registration centres in the Country and has since 2012 registering and identifying Citizens, Refugees and Legal Resident in Dar es Salaam and Morogoro Regions[7]. Up to the end of 2012, NIDA has also successfully registered almost all Government Employees residing in the Dar es Salaam region and started issuing them with Identity Card immediately after the launching of the first Identity Card by the President of the United Republic of Tanzania and finally making the dream tangible.[8]

At this stage where NIDA has managed to register and issue to all Government Workers[9] with National Identity cards and have so registered all Dar es Salaam

---

[5] Ibid, at P.49

[6] National Identification Authority of Tanzania was established by virtue of **Article 36** of the Constitution of the United Republic of Tanzania of 1977, under **G.N 122 of 2008**

[7] *See* www.nida.go.tz

[8] The first National Identity Card was issued to the President of the United Republic of Tanzania on 7th February, 2013

[9] *See* **http://m.dailynews.co.tz/index.php/local-news/15482-muhimbili-employees-get-national-id-cards** **NIDA** distributed National ID Cards to about 2000 Muhimbili Refferal Hospital as part of the initiative to provide Government Employees with the National Identity Cards

Residents to date, it is now undeniable fact that there is an immense amount of information extracted from the people within this Jurisdiction, where Identity cards are now in the wallets and handbags of various people in Tanzania which call for an effective mechanisms to protect such information from any abuse or improper use. This therefore calls for the need of Data protection initiatives. Privacy concerns has not been an exclusive matter to Tanzania at times of introducing or implementing National identification systems, but a common place to other countries around the world. In other jurisdictions, in Britain for example, it has been argued as follows;

> *" ... Alongside this concern for the possible constraints on civil rights or on democratic political involvement is another, for personal privacy. Many opponents of ID cards feel that they constitute a further unwarranted means whereby alien agencies may intrude or invade a personal sphere. The problem is that personal data may circulate more freely when an ID card system is in place, simply because, without careful regulation, the channels are that much more open.*
>
> *The British Data Protection Act gives only limited protection against the unauthorised disclosure of information from a computer file to other persons or organisations. Nearly all local authorities already sell copies of the Electoral Register to commercial bodies, and it was envisaged that the football ID system would do the same, so it would appear that this fear is justified...."*[10] .

[10] Lyon David, **"British Identity Cards: The unpalatable Logic of European Membership?** at P.383.

1.2 Statement of the Problem

In Tanzania of today, registration of Citizens, Refugees and Legal Residents is inevitable. The Law requires each one at the age of eighteen to register himself with the National Identification Authority (NIDA) so as to get the National Identity card. As explained in the preceding part of this Chapter , this exercise results into the extraction of immense Information from all persons in Tanzania which now calls for another measure to protect them from any sort of abuse with the idea of privacy in mind.

It has been further stated that, the long term vision towards the design and development of National ID is that The National ID must provide the foundation to position itself to participate in the e-Government information exchange Networks. The National ID system is part of a larger vision that will further enable integration with other national wide Governmental and Administration systems as well as be the starting point for secure access and usage of forthcoming e-Government services in Tanzania[11] . The Spirit of the e-Government Information Exchange Network is to facilitate a sharing of common systems and Infrastructure to provide for optimal utilization of resources with increased efficiency[12] .

The above vision clearly emphasize the emergence of a situation where NIDA would act as Central Unit to enable integration of various Government and other Administrative and private businesses to work together. This may happen for example, when an individual applies for personal Loan from a Bank, the latter may

[11] Gotham International Ltd, (2006**),op.cit,** at P.104
[12] **Ibid**, at P.105

enquire from NIDA for the genuineness of the information that this individual has submitted to the Bank.

Therefore, this state of affair creates a need for a study to assess the existing Legal framework providing for the Data protection and privacy issues, if any, and identify the lacunas and access the implications of the said lacunas on Data Protection Legal Regime to the current situation in Tanzania where the National wide exercise of registering and identifying people has already taken charge, and recommend accordingly.

1.3 Research Objectives

The researcher will be guided by the following General and Specific objectives:

1.3.1 General Objective

The Main objective of this research is to examine the existing Data Protection Legal Framework regime in Tanzania in connection with the registration and identification of persons exercise in Tanzania.

1.3.2 Specific Objectives

Specific objectives of this research include:

2 To identify lacunas/gaps in the entire Legal Framework for Data Protection in Tanzania.

3 To assess implication of the gaps in the Data protection Legal Framework in Tanzania.

4 Recommend ways of improving the Data Protection Legal Framework Regime in Tanzania.

a) Research Questions

The research seeks to answer following general and specific questions:

General: To what extent does the existing Data Protection Legal Framework Regime protect the Data Subjects whom are registered with NIDA?

Specific: What are the lacunas/gaps in the existing Data Protection Legal Framework regime in protection of Data Subjects registered with NIDA?

What are the implications of the shortcomings in the existing Data Protection Legal Framework regime in protection of Data Subjects registered with NIDA?

b) Significance of the Study

Conclusion and recommendation to be drawn from this study include the following significance;

1. Analyze existing laws, identify lacunas/gaps and advise the Tanzania Government and Tanzania Identification Authority on how to improve the existing Policy, Laws and Regulations in improving Data Protection Legal Framework.
2. The Findings of the Research will be useful input to Law Makers, Academicians, Potential Researchers and other actors dealing with identification and registration of persons, privacy matters and Data protection issues at large. It will enable National Identification Authority (NIDA) to better protect its Databases and

general information during interfacing activities with other stakeholder. The Study will shade light on this aspect.

1.4 Research Design and Methodology

1.6.1 Area of Study

The researcher has chosen the National Identification Authority (NIDA) as the case study for the research for the following reasons:

i. It is the only Government Institution mandated to handle all registration and identification of persons and therefore has all necessary information regarding Registration and Identification laws, policy and management of National Identification system.
ii. It is an Authority which has upper hand regarding enactment and amendment of policy and regulations relating to registration and identification of persons in Tanzania.
iii. Geographically it is convenient for the Researcher to collect data since the Researcher resides in Dar es Salaam

1.6.2 Research Data

All kind of data primary, secondary and tertiary data has been collected in order to get good composition for the research.

1.6.2.1 Primary Data

Primary data were collected through observation of the various activities related to registration and identification of persons in Tanzania.

1.6.2.2 Secondary Data

These data were collected from the Legal Directorate and Directorate of Identity Card Management which deals with the registration and Identification of persons. The Researcher expects to receive data through available documentation.

1.6.2.3 Tertiary Data

These are Data that have been obtained from National Identification Authority of Tanzania (NIDA) publicized articles such as Authority Establishment Instrument, Authority profile, Feasibility Study Report and through their website (www.nida.go.tz). The available data will help the researcher to write the research paper with quality data and also minimize the time consumption during data collection.

1.6.3 Data Gathering Methods and Techniques

Various methods of data collection were deployed so as to get the best information which has enabled the researcher to analyze the data. Those methods include; Literature review, Observation and documentary review.

1.6.3.1 Documentary Review

Authority Documents has been reviewed which will assist in clarification of some data. Documents relating to Data Protection in the National Identification Regime will be reviewed.

1.6.3.2 Observation and Informal Discussion

The Researcher has also used the observation technique in the case study in order to get data. This will help in situation clarification.

1.6.3.3 Literature Review

Literature regarding Data Protection in the National Identification Regime was reviewed and important information retrieved has assisted in explanation of finding.

1.6.4 Validity and Reliability

A combination of different methods such as interview, questionnaires, documentary review and observation in collecting information has been employed to back up and complement on each other to bridge the weakness of each method.

1.6.5 Data Analysis Procedure

Both qualitative and quantitative data analysis technique has been used to analyze data collected.

a. Scope of the Study/Research

The study has analysed existing Policy, Laws and regulations in support of Data Protection Legal Framework and how the said laws, policy and regulations can be improved to protect Data so far collected in the National Identification system in Tanzania.

This study will centre on the National Identification system at large and the National Identification Authority Headquarters at Dar es Salaam as the case study.

b. Limitation of the Study

Putting into consideration limited time, finance and response of the Public to the Questionnaire, the Researcher faced few challenges likely limited the effectiveness of the research to a more satisfactory standard.

c. Delimitations of the Study

The study was confined in National Identification Authority of Tanzania. Data has been collected from the staff of the Legal Directorate, ID Cards Management directorate and Information systems Management Directorate. Also, the research data collected will be those relating to Data Protection and privacy issues in the National Identification system.

CHAPTER TWO

2.0 THE EVOLUTION, CONCEPT AND FUNCTIONING OF NATIONAL IDENTIFICATION SYSTEM

This Chapter looks at the genesis of the National Identification system in the various parts of the world and Tanzania in particular and how this system works. It also observes how to different perceptions have been experienced in different parts of the world as to why they decided to introduce National Identification systems.

2.1 Evolution and Motivation Behind the Introduction of National Identification Systems in Various Parts of the World

For almost two decades now, the world has witnessed the mushrooming of the introduction of National Identification systems around the world in various Countries in Europe, Asia and some of the Latin America. Before embarking into the operability of the National Identification system, it will be of great importance for purposes of understanding, to first know the motivations behind the introduction of National Identification Systems in various Countries around the world, and all, during the same era in time.

The advancement in the technology has an upper end at great impact. Technology in never and has never being static, but ever changing. This changing nature of Technology has brought about many influences on various disciplines including that of National Identification systems.Previously, one was only identified by demographic Data only unlike the recent deployment of the Biometric technology[13].

[13] *See* **Article 29** of Data Protection Working Party and the European Data Protection Supervisor whom have opined widely on the use of Biometric data.

This development poses a challenge of on the whole undertaking of identifying an individual. This has long been acknowledged by various writters as follows;

> *" As far back as 1993, long before the internet became commonly used by the general public, the New yorker Magazine published a now well known Cartoon by Peter Steiner of two dogs sitting in front of a computer workstation. One Dog says to the other 'on the Internet, nobody knows you're a Dog'. This could be seen as an example illustrating the challenges faced in proving one's identity in a distributed systems environment"*[14].

The dangers posed by this constant innovations in the Technological sphere, truly make it harder to identify someone or even connecting him with a certain act which he has commited online by using a Computer via Internet.The National Identification Systems is there inevitable on solving this emerging challenges. The use of the biometric for example, can enable to tell who used which Computer and at what time. If one uses a Computer, for exaple to create a Document which will scandalise his own Institution upon its Publishing, and if he is clever enough not to connect in that particular Office LAN, then it is still easy to trace this person by tracing the finger prints he might left on the keyboard of the Computer he used.

Another influencing Factor is the emergence of terrorist activities at the Global scale. US Embassies in Tanzania and Kenya were bombed by suicide attackers killing people and leaving many other with severe wounds followed by the bombing of American twin towers of the World trade Centre in September 2001.

---

[14] Arora, S., (2008), **" National e- ID card schemes: A European overview"**, *Information Security Technical Report 13*, 46-53

Figure 2.1: The Peter Steaner Cartoon can be elaborated as follows[15];

These two major incidences completely changed the life styles of almost many parts of the Globe and how varous matters are dealt with and even on new methods of identifying people. There emerged a need to come up with the mechanism or system which would enable people to be identified with accuracy in order to capture the perpetrator of any future event ofsimilar nature[16].

India on their part, tries to establish major surveillance projects out of which the main one is the introduction of the Unique Identification Number (UID), the development of which has commenced under the Unique Identification Authority

[15] Stener, P., (1993), The New York Magazine.
[16] *See*, Gotham International Limited (2006) **"Feasibility Study Report on the Registration and identification of persons",** at P.49

(UIDAI) of India. UIDAI with the principal mandate of allocating about 1.2 Billion Indians was established in February, 2009[17]. In USA, it has been argued on various occassions that the September 11th attack has some significant impact on the way America should approach security matters especially on how to closely identify the immigration movement of people in and out of the States. This is vivid as follows*;*

> *" Because of the terrorists who carried out the September 11 attacks were known to be security risks or had visa violations and still were able to spend months undetected in the United States while traveling, attending flight schools, and renting apartments, proposals for creating a national identification card system have gained new attention"*[18].

The case with the United Kingdom is that, the United Kingdom Parliament passed the Identity Cards Act in March 2006.However, the scheme faced a lot of opposition from various interesting groups each having its main concern. For example, the Information Commissioner was quoted saying;

> *"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far moer people shared across many more boundaries than British society would feel comfortable with"*[19].

However todate, the Identity card in Britain is not compulsory but merely voluntary since massive opposition regarding the cost of the project and the likely,as to the belief of many Britons, infringement to the privacy of the people.The National

---

[17] Greenleaf, G., (2010), **"India National ID system: Danger grows in a privacy vacuum"**, *Computer Law & Security Review 26*, 479-491, Elsevier Ltd, at P.1.
[18] The Century Foundation, **The Debate over a National Identification Card**, P.1
[19] *See* **the Times News Paper** of August 16th, 2004

Identity Register was destroyed in 2011 by the Home Office under the coalition Government of Conservatives and the Liberals[20]. Apart from the security concerns and counter terrorism measures as among reasonns for the introduction of National Identification systems, there are other good reasons for such establishing the identification system. In this area, Tanzania National Identification Authority (NIDA) may set a very good example in this category.

Harmonising the main Government machinery forms a key reason behind establishment of the National Identification system in Tanzania.For example, when a crime is commited by a person here in Tanzania,the Police force face challenges on collecting facts and clues so as to establish strong evidence against the alleged crime. This is mainly caused by the lack of identity of the suspect who commited such crime.If this person is registered and well identified through the National identification system, it is easier to trace and capture the suspect as one of the infromation required during the registration of every Tanzania is the adress of the residence of the Applicant. Also the photograph and the fingerprints of that person.

If these details about an individual is captured, and especially fingerprints for example, it is easier to trace this person given the fact that a suspect tend to leave his traces during the commisioning of the crime.One may leave the fingerprints when touching items in the crime scene for example,if this person is registered and his fingerprints forms part of his identity in the National population register, it is easier to trace this person in the vicinity unlike when this person's information is not

[20] *See* **http://en.wikipedia.org/wiki/Identity_document#United_Kingdom**

registered. This is well demonstrated during the feasibility study in Tanzania as follows;

> *"ID card could provide an invaluable tool in the fight against crime. The feasibility study proposes the creation of a Biometric Database which could assist the Police to link crimes to the perpetators. Assuming all eligible citizens are registered in the National Biometric database, fingerprints obtained from a crime scene could be used to conduct a fingerprint match on the National database which could be a very useful tool in combating crime"*[21].

National Identity Card is also used as an identity of one's Nationality. This move therefore is one of the way of guaranteeing individuals of this Internationaly recognised right to Nationality which has been stated in various International Instruments and other decided case at the international forum. This notion can be justified by the Inter-American Court of Human Rights which affirmed that Nationality is the legal bond that guarantees individuals the full enjoyment of all human rights as members of the political community.Although States maintain the sovereign right to regulate Nationality, States' discretion must be limited by International human rights standards that protect individuals against arbitrary State actions[22].

At the International Level, the right to Nationality has been provide for by various Conventions as follows;

---

[21] See, Gotham International Limited (2006), **supra note 5**, at P.10
Also see, Kent T.S., et al, (2002), **"IDs—Not That Easy: Questions about Nationwide Identity Systems"**, National Academy of Sciences, National Academy Press, Washington, at P.6

[22] *See* the **Case of Dilcia Yean and Violeta Bosico .V. Dominican Republic [**Inter-Am Ct. H.R., (Ser.C) No.130 (2005)]

On its side, the **Universal Declaration of Human Rights**[23] on the right to Nationality has the following to state;

"1. Everyone has the right to a nationality.

2. No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality"[24].

Further, **International Covenant on Civil and Political Rights (ICCPR)**[25] has recognised the right of Children to their fundamental rights as to the Nationality and Citizenship.it states that;

> "Every Child shall have a right to acquire Nationality"[26]

Another Convention is the **Convention on elimination of all forms of discrimination against women (CEDAW)**[27]. Here, women are quaranteed equal rights with men regarding the Nationality of the children.It states that;

> *"States Parties shall grant women equal rights with men to acquire, change or retain theirnationality. They shall ensure in particular that neither marriage to an alien nor change of nationality by the husband during marriage shall automatically change the nationality of the wife, render herstateless or force upon her the nationality of the husband. 2. States Parties shall grant women equalrights with men with respect to the nationality of their children".*

---

[23] Adopted by United Nations General Assembly in
[24] *See* **Article 15** of Universal Declaration of Human Rights.
[25] Adopted by **UN General Assembly** on 19th December, 1966 a*lso available* at **http://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf**
[26] Provided under **Article 24(3)**
[27] Adopted by **United Nations General Assembly** in 1979

Convention on the rights of the Child[28] has also enshrined this right as to Nationality to Children and quaranteed them of security against any illegal deprivation of their right to identity.The provisions reads as follows;

> *"1. The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.*
>
> *2. States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under the relevant international instruments in this field, in particular where the child would otherwise be stateless"*[29].

Another main reason in Tanzania for establishing the National Identification system is the urge to control illegal immigration. Tanzania is bordered by quite a big number of Countries making its Immigration Office one of the busiest Office on Land. These Countries include Mozambique Malawi and Zambia on the South Eastern part, Democratic Republic of Congo, Rwanda and Burundi on the Western and Northern Western part, Uganda and Kenya on the Northern Part. Large part of Tanzania Eastern is the Indian Ocean and one of the longest shores stretching to about 1000Kms from the Cost of Tanga to that of Mtwara, the areas which are also porous to immigrants from the war torn Nation of Somalia. In this Area, the feasibility study conducted in Tanzania states as follows;

"Tanzania is surrounded by Countries that are relatively politicaly unstable

[28] Passed in 1989
[29] **Under Article 7**

and have been so far over half a century.Every few years or so there are civil wars in the bordering state of Rwanda, Burundi and the Democratic Republic of Congo. Each time these internal wars flare up, Tanzania is inundated with refugees crossing our borders in search of safety and shelter. Some of the Refugees have overstayed their welcome by mingling with the locals and in the absence of the identity cards it is difficult if not impossible to separate the Refugees from bona fide Citizens. This could have undesirable consequences especialy during elections when illegal immigrants could negatively influence local and national elections[30] *".*

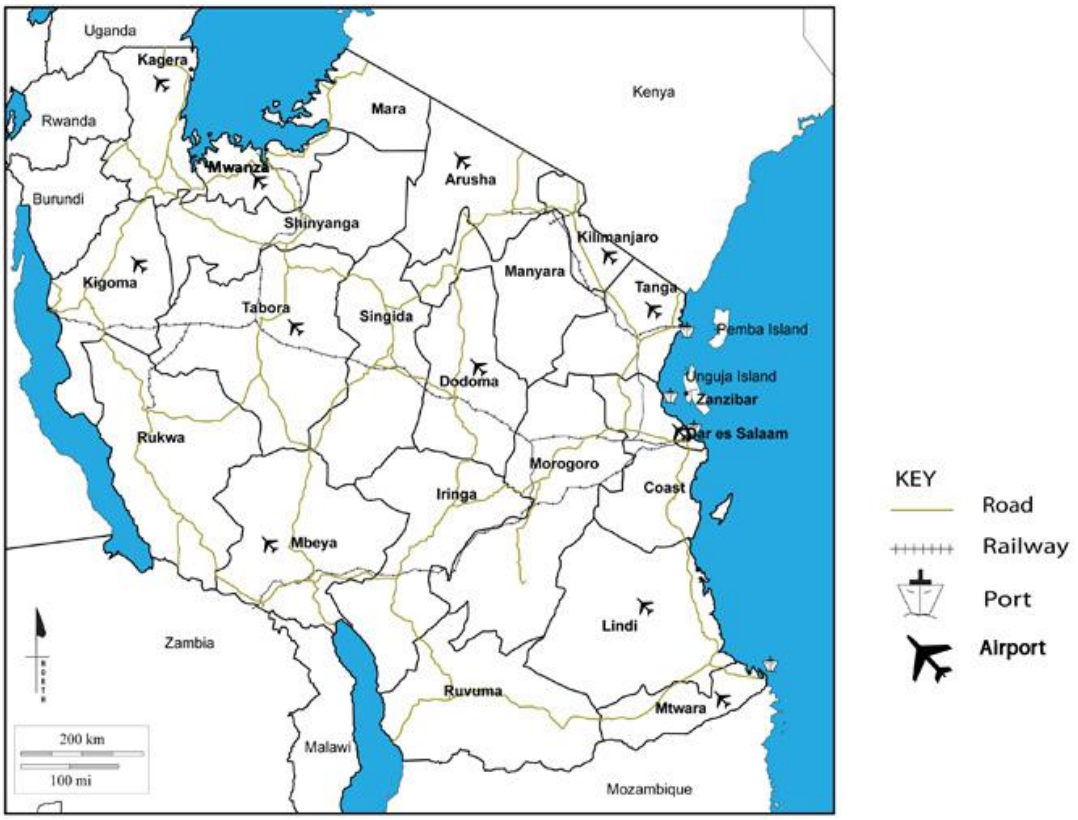

Figure 2.2: Tanzania Map Showing The Bordring Countries[31]

[30] **Supra Note 5**, at P.11
[31] Available at https://www.google.co.tz/search?q=tanzania+map+showing+bordering+countries&tbm

Further, streamlining Government operations forms part as to why National Identification system was formed in Tanzania. In Tanzania since the beginning of the year 2000 onwards, the Government commited itself on establishing the e-Government so as to cope with an ever changing nature of technology. To effectively achieve this, the Government adopted the Information Communication Technologies (ICT) Policy[32] in order to state that in the Government major Poicies and formally recognising e-Governance it in the ICT Policy.

Tanzania National Identification system has been formed on the foundations and platform of the Information and Communication Technologies Platform and the objectives.The National ICT Policy in recognising this it states as follows in its Policy objectives;

> *"Foster efficient, inter-operable, reliable and sustainable national ICT infrastructure commensurate with grass-root needs, and compliant with regional and international standards, with increasing access while reducing cost*"[33].

In working under these parameters of the ICT Policy, the streamling of the Government operations was inevitable as the adopted ICT Policy required it to be done that way. Consequently the introduction of the National Identification system was exactly in line with the introduction and the requirement of the creation of the inter-oprable systems of the Government.The Feasiblity study also championed this move by stating that;

---

[32] *See* **Information and Communication Technologies Policy of Tanzania of 2003**, at P.5
[33] **Supra note 32**, at P.9

> *" The use of the Information and Communication Technology in public administration, also known as e- Government, has been embraced by the Government of Tanzania and its partners in the EAC and SADC.e-Government combined with organizational changes and the introduction of new skills in public Institutions is intended to improve public services, streamlining Government bureaucracy, enhance the democratic processes, strengthen support to public policies, and increase accountability and productivity"*[34].

The National Identity system has other multiple advantages depending on the use and need.In the United States for example, nationwide identity systems have been sought for many purposes in addition to countering terrorism. They have been proposed to aid in fraud prevention (for example, in the administration of of public benefits), catch *deadbeat dads* enable electral reforms, allow quick background checks for those buying guns or other monitored items, and prevent illegal aliens from working in the United States[35].

In other jurisdictions, the European Union being the key illustrating area, the introduction of the certain elements of the National Identification system was a result of certain legislative undertakings within the European Union.In order for those Directives to be implemented, then certain systems were to be established. For example, in 1999 the european Directive on Electronic Signatures was passed which lead to national legislation to be implemented by each member state. Initiatives at

[34] **Supra note 5**, at P.11
[35] **Supra note 10,** at P.383

both the pan-European and national levels were started to enable this directive could be reaslised.Specifically, an e-ID card with a built-in smart card was seen as the necessary Secure Signature Creation Device (SSCD) as defined by the EU Directive[36].

With the above analysis, one would realise that, the coming into being of the National Identification system in various Countries around the world including Tanzania, was nor accidental, they were coupled by the number of factors which range from technological to security issues,the urge to improve functioning of certain Government and private systems (the interoperability of certain Departments within the Government and also in the Private Institutions) and to a large extent as a result of certain Legislative measures (Example, the European Directive on electronic Signatures).

2.2 The Concept and Functioning of The National Identification System

2.2.1 National Identification Authoriy (NIDA) of Tanzania as Case Study

For the proper understanding of the concept of the National Identification system, it is of paramount importance to observe the structure and the operations part to it for purposes of knowing and understanding it. Generally, **National identification system** is a computer based system where personal information of an individual is associated with the unique identifier (ID Card) while this particular information will be stored in the central Data base[37].

---

[36] **Supra note 3**, at P.46

[37] Froomkin M., A., (2004), **" The Uneasy Case for National ID Cards",** *University of Miami School of Law*, at P.1

Further, **Identity** is a set of information about a person.National Identity number is a tool that permits the bearer to prove in a high degree of certainty,that they are who they say they are.The number provided certainty because of the security around its issuance and the technology used in its presentation.It must not be confused with they name (which is just one of many attributes) or their means of identification. Everyone has many identities potentialy one for every relationship they have in which they disclose different subsets of their personal information. For example, work related identities are mainly about their roles in the workplace.One's identity as seen by his/her friends are mainly about his/her leisure activities.One's identity at his or her Bank consists his or her financial information.

On the other side, a **Physical Identity Card** in identifying token that contains a unique identifier. The unique identifier links the holder to Databases. The card may also contain various tyypes of stored Data that facilitate the authentication of the legitimate holder of the ID, or facts about her.The Virtual ID Card is not even that-it is just an index number stored somewhere, or likely many somewheres, that matches attributes of a person (e.g Biometric identifiers) to one or more collections of data[38].

It is sometimes argued that, the analysis of any national identification scheme requires attention to all aspects that contribute to it, including (at least) the number, the biometrics and other identification data collected, the undelying computer system, the tokens (cards or others) carrying the number, the uses to which it is

[38]Froomkin M., A., (2004, **Supra Note 37** , at P.4

permissible to put the number and the tokens, and the parties who are allowed to participate in any aspect of the system's operation[39].

For the case of the National Identification Authority of Tanzania,There is a *Client enrolment terminal*. At this point is where the information of the Client is captured. Is actualy where NIDA meets face to face with the Clients and deliver the service it is mandated for.Is used to by the National ID Agents to collect Client to Data and biometric information before the information is uploaded into the National Data Registry and Biometric Database[40].This is the Office deployed at the Regional to District Level.

Another part forming this system is the *Client verification Terminal*.Is also the Office deployed at Regional to District Level.This Office is used to collect Clients demographic and biometric data in order to perform identity verification.Later, the information captured here is compared against the registration Data contained in the National data Registry[41]. Further, *personalization system* is also established. This is the central system that is used to customise and print the ID cards as the last processing step in creating secure ID cards. A personalisation system consists of a Desktop computer with specialised personalization software and a personalisation computer for printing the ID cards.Also included in the personalization system is a QC workstation required for quality control[42].

[39] Greenleaf, G., (2010), **supra Note 6,** at P.480
[40] *See* Gotham International Limited, **Supra Note 5** at P.12
[41] *See* Gotham International Limited, **Supra Note 5,** at P.12
[42] **Ibid**

The *virtual private network* also forms the National Identification system of Tanzania.This is the Nationwide telecommunications network infrastructure that provides the connectivity between the Client enrolment and the verification Terminal and the National ID Data Center where all the Data processing is performed. Since the enrolmennt and verification terminal may be located at a remote border outposts or small village or in a mobile truck, different virtual private networking technologies will be required to meet the unique requirement of a particular setup[43].

Lastly, the type of Technology to be used to make an Identity Card is also a point of consideration. However, this is a matter of choice of the Country in question. The two leading ID technologies extensively investigated for the National ID project are 2D Barcode and Smartcard. While 2D barcode technology has been widely used for applications ranging from Driver's licence and voter registration cards, it has become apparent that the technology is not secure enough for an important application like the national ID program. 2D barcode information can easily be read and copied on another card using a simple $ 500 computer with easy to obtain software[44].

Tanzania National Identification Authority NIDA has decided to adopt the smart card technology in its Identity Cards so as to cope with technological advancement and not to lag behind[45].

---

[43] **Ibid**

[44] *See* Gotham International Limited, **Supra Note 5,** at P.12

[45] The Identity Card the President of the United Republic of Tanzania inaugurated in February, 2013 was built on the smart card technology which to date is among top level technologies.

2.3 The Legal Status of the National Identification System in Tanzania

The current National Identification and registration of persons system in Tanzania is executed under the mandate provided for by the Regisration and Identification of persons Act[46].However, the implementation of the National ID program is implemented almost twenty (20) years after the enactment of Registration and Identification of Persons Act in 1986.

The Act was never in force until when it was enforced under **GN 257A of 26th August, 2011**.This was possible three years after the establishment of National Identification Authority (NIDA) in 2008[47] when it got into full fledged implementation of the National ID project. Let me now criticaly analyse the main features and the shortcomings of the Registration and Identification of persons Act as compared to the current prevailing circumstances;

All activities so far related to the registration and identification of persons in Tanzania are executed under the mandate of the Cap 36 of the Laws of Tanzania as revised in 2012.This Act for example, provide for the following regarding the implementation of National Identification programme in Tanzania;

It provides for a person eligible for registration and qualifying to get a National Identity Card in Tanzania. It has categoricaly pointed out that a person of the age of eighteen years old or above is the only group of people who stands a chance of being registered and later being provided with an Identity card.It states as follows;

---

[46] **Act No.11 of 1986** which is now **CAP 36 R.E 2012**
[47] Under the auspices of **NIDA establishment Instrument of 2008**

> *"Subject to subsection (2) and other provisions of this Act, every person of or above the age of eighteen years who, on or after the commencement of this Act, is or resides in the United Republic and to whom this Act applies may make an application for registration in pursuance of this Act"*[48].

Further, it also provides for the types of the identity Cards to be provided to the registrants. The Law has categorised the applicants into two major groups being the Citizens, the Legal Residents .All these groups will be provided each with a special type of card depending with the respective group that the individual belongs.This matter is provided for as follows;

> *"There shall be two types of identity cards of such form as the Minister may prescribe in respect of; (a) citizens of the United Republic; (b) aliens resident in the United Republic; and an idenity card shall contain such particulars to e precribed as may be necessary for the purposes of identifying the holder"*[49].

And of more importance, the Act has provided for the procedure on how the registration process should take place and which type of particulars should be taken from the Applicant of the National Identity Card in Tanzania[50]. The Law has also provided on other main issues including the issues of Offences and Penalties, replacement of Identity Card, duty to walk with the Identity card and the Powers conferred to the Minister on making a Regulation[51].

---

[48] **S.7 (1)** of Cap 36 R.E 2012
[49] *See* **S.10 (1)** Ibid
[50] *See* **Supra Note 46**, S.9
This Act has stated particulars required to include Name, Address, Nationality, Birth Place, Age, Sex, Marital Status, Profession and such other Particulars as the Minister may direct.
[51] *See* **Part III & IV** Ibid

However, given the timing of the enactment of the Act and the technological status of the at the time of enactment of the Registration and Identification of persons Act in 1986, there are so many shortcomings within the Act inviting for the major reviews withing various sections of this law.This paper will review some of those shortcomings.

Firstly, it immensely empowers the Minister responsible for the supervision of the National Registration and Identification of persons whom is the Minister of Home affairs. The powers of the Minister enshrined in the Act inlcudes;

To appoint as to when the Act may come into operation. In this part, the Act provides as follows;

> *"This Act shall come into operation on such date as the Minister may, by notice published in the Gazzette, appoint"*[52].

Another power is that of appointing Officers to work in the National Identification Authority.The Act states that;

> *"The Minister shall, appoint by name or Office a public Officer to be the Registrar for the purposes of this Act"*[53].

Further, establishing or setting up such Offices necessary for implementing the Act. This is provided as follows;

> *"The Minister may, establish or setup such Offices as he may deem neccessary for the purposes of this Act, and may appoint an Officer to be known by such style as he may determine, to have charge of each of such*

[52] **S.2** ibid
[53] *See* **Supra Note 46,** S.5(1)

Office"[54].

Moreover, to determine terms and conditions of service of registration Officers. The Act provides that;

> *"Subject to subsection (2), Registrar and every other registration Officer shall hold Office upon such terms and conditions in relation to his Office as the Minister may determine"*[55].

However, on the same issue the law has given exception to the general rule above as follows;

> *"Where any registration officer is appointed to such Office under this Act, by reason of his holding any other office in the Civil Service, he shall hold such office for such term and upon the conditions under which he continues to hold the first Office"*[56].

All these powers if criticaly observed means that, the National ID program would therefore not work unless the Minister executes the necessary statutory duties and powers conferred to him by the Act. Further, powers of the Minister to appoint inlude power to dismiss.Likewise the powers to establish inlude power to close down. And also to determine powers and duties of the Registrar and any other Officer in the implementation of the Registration and Identification of Persons Act.The law states that;

> *"The powers and discretions vested in the Registrar and assistant registrar may be excercised by a registar, assistant registar,immigration officer or any*

[54] Ibid, **S.5(4**)
[55] Ibid, **S.6(1)**
[56] Ibid, **S.6(2)**

other public officer as the Minister may, by notice published in the Gazzette, specify"[57].

With the above provision however, one thing not clear is the intention of this provision.If it is intended that the Minister may appoint a public Officer to be a registration Officer under this Act, but without separate remuneration for this additional responsibilities, then the intention to limit expenditure of resource in the National ID program would definitely be counter production.

At large, the Registration and Identification of persons Act of 1986 is now almost 27 years old and considerably taken by events and of more significance is not featured in the current massive advancement of in the field of Information and Communication Technology (ICT) of which is a platform on which the National Identification system has been formed not only in Tanzania, but in almost all Countries aorund the world which has decided to establish and implement the National Identification system.

And finaly, the Law has not at all ventured on the issues of *Data protection* or any *Privacy issues* regardless the fact that it has directed for the registration and identification of persons which automaticaly would lead to immense accumulation of personal Data of persons in the United Republic of Tanzania. On the other side, the National Identification Authority of Tanzania is not a creature of the Registrationa and Identification of persons Act of 1986.This Act did not establish National

[57] *See* **Supra Note 46,** S.5(3)

Identification Authority (NIDA) but only mentioning the Minister responsible with identification issues as one to run all related affairs with National Idenitification system[58].

Conclusively, the introduction of National Identification system was highly motivated by a number of factors as described above which range from security reasons, enhancing the Government functioning, execution the requirement of the Information Communication Technology (ICT) Policy and the desire to identify people residing in the respective Country.For the case of Tanzania, the National Idenfication programme is executed under the mandate of Registration and Identification of persons Act of 1986 as revised in the year 2012.On the other side, Tanzania National Identificaion Authority (NIDA) is the Institution in Tanzania mandated to implement the National Identification programme and therefore turn to be the executor of the said Act.

[58] NIDA has been established by the President of United Republic of Tanzania under **Establishment Instrument of 2008** by powers conferred to him by **Article 36 (2**) of the Constitution of the United Republic of Tanzania of 1977 as amended.

CHAPTER THREE

3.0THE EVOLUTION, CONCEPT AND THE LEGAL FRAMEWORK FOR DATA PROTECTION AND PRIVACY: THE EUROPEAN UNION IN PERSPECTIVE

In this part of the Dissertation, the Data protection and matters relating to Privacy are examines and discussed. This includes the Development of the Data Protection and Privacy issues and the main Concept behind Data Protection. This will help to understand the need for Data Protection and Privacy Issues and therefore able to understand the challenges which may be faced in the absence of the firm and sound Legal framework for Data Protection and Privacy.

3.1 The Evolution of Data Protection and Privacy

The Data protection and the privacy issues received paramouncy even before the thinking of establishment of National Identification systems has come into the level of the idea.The main concerns of the Data protection dates back far during the establishment of the United Nations in 1945. Its establishment did associate also the introduction of other Agencies championing for the Human rights.

On 10th December, 1948, three years after the lapse of the World War II, many Nations joined hands in support of the declaration of Human rights as fundamental and inherent right to all the peoples of the world. Regarding privacy, the Universal Declaration of Human Rights states that;

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*

Everyone has the right to the protection of the law against such interference or attacks''[59].

This incredible step in the in the Human History, had created tremendous positive impact to most Nations which ratified it not only on issues relating to privacy but on other matters that it comrehensively provided for.So it was somehow the begining of other enectment and recognition of the Human righst on the area of Data protection and privacy at large.

At National level, few Nations exclusively legislated in favour of Data protection at their local jurisdiction. German and Sweden can set a very good example in this.German on their side decided to, though just at the State of Hesse which adopted the world first Data Protection Statute in 1970.The first National Statute was the Swedish Data Protection Act of 1973[60].

On recent years, many Countries have embarked a lot of efforts in the recognising right to privacy and even adopting various measures on making sure personal Data is in no way abuse for whatever purpose during its processing.The abuse of Data during processing is the actual cause of the infringement of privacy of an individual whose Data has been finaly abused.

At this juncture, though similar issues were at hand to various Countries, their approach to solve them differed.Within Europe, omnibus data protection legislation

---

[59] *See* **Article 12**
Also See Lloyd,J.I., (2011), **"Information Technology Law",** 6th Ed.,Oxford University Press, Great Britain, at P.12

[60] **Ibid**, at P.22 for the case of German, all legislative initiatives on Data protection happened as one of the measure of deterring the Data misuse similar to that which happened during the World War II under totalitarian Regime.

has been the norm, covering all aspects of processing personal data.In the United States and perhaps the majority of the countries in the world, a sectoral approach has been favoured, with a range of so called, privacy protection statutes being enacted to regulate specific forms of information handling[61].

These initiatives never ended only at the National level, some International initiatives regarding Data protection were under way and the finaly came into being.In the Data protection context, perhaps two concerns prompted International action. There were fears that National laws, which tended to have strong controls over the export of data might have a protectionist effect. Conversely, there were fears by those States that had adopted data protection legislation that national laws and policies could be circumvented by organisations sending data abroad for processing in countries often reffered to as data havens which imposed few controls over processing activities[62].

The major Data protection initiatives at the International forum is mainly a result of the efforts by the European Council and the Organisation of Economic Corporation Development (OECD)[63].The European Union on their side had came up with the European Convention on Human Rights. As more and more European Countries enacted data proitection legislations, so too did the problems resulting from the international trade of information, frequently reffered to as transborder data flows become more acute.In an effort to minimise restrictions on the free flow of

[61] Lloyd,J.I., (2011), **supra note 39**, at P.21
[62] **Ibid** at P.23
[63] Is an Organisation responsible for facilitating cooperation between Member States in order to promote economic development.

information, and in the hope of preventing major descripancies between the national data protection laws, the Council of Europe moved beyond its earlier recommendations to sponsor the Convention[64] for the protection of individuals with regard to the automatic Processing of personal data[65].

On the other side, the OECD's work in what it has tended to refer to as the privacy protection field began in 1969 when a group of experts was appointed to analyse different aspects of the privacy issue,e.g in relation to digital information, public administration, transborder Data flows, and policy implications in general[66]. Further, the right to privacy is prime in the European Community paying attention to its recognition in the European Convention for the protection of Human rights and the fundamental freedoms.This Convention has stated that;

> *"Everyone has the right to respect for his private and family life, his home and his correspondence AND; There shall be no interference by a public authority with theexercise of this right except such as is in accordance with thelaw and is necessary in a democratic society in the interests ofnational security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"*[67].

Protection of personal data is agin recognised in the European Community under the Charter of the Fundamental right of the Fundamental rights of the European

[64] This Convention entered into force in July, 2004
[65] Lloyd, J.I., (2011), **supra note 59,** at P.25
[66] Lloyd,J.I., (2011**), supra note 59**, at P.27
[67] *See* **Article 8 (1) & (2)**

Union[68].The Charter[69] has clearly without anny hesitancy stated as follows;

> *"Everyone has the right to the protection of personal data concerning him or her; Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified AND Compliance with these rules shall be subject to control by an independent authority"*[70].

The provisions of the two Conventions above make it evident how sensitive it is when it comes to how should personal Data be treated and the exclusive right that a person coming form a Country which is a member of the European union is granted on his personal life and even the none provision of such information without the knwoledge of the person possessing such information.

There are some decision in the European Union which were made in favour of those struggling to protect their privacy under the provisions of the two Conventions above and proved the serious of the Courts in the Eu on implementing these rights. One of such case is the case of ***Sciacca V. Italy***[71]**.** In this case, the Applicant, Mrs Sciaaca, an Italian Teacher at the private school in Lentini sought form the European Court of Justice for the compensation regarding the misuse of her photographs which was released during the press conference after being organised by the Public prosecutor's

---

[68] *See* **the Official Journal of the European Communities** (2000 C 364/01)
[69] Of **18.12.2000**
[70] **Article 8 (1), (2) & (3)**
Also ***see*** **Article 7**, which recognises right to privacy.
[71] Application no. 50774/99 of 2005 decided by **the European Court of Human Rights.**

Office and the Revenue Police and that this act amount to the infringment of her right to respect for her private life[72].The Applicant relied on Article 8 of Convention which is worded as follows;

1. Everyone has the right to respect for his private and family life, his home and his correspondences.
2. There shall be no interence by a public authority with the excercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of National security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

In adressing whether the Applicant's right was infringed, the Court decided to answer each requirement or condition set out under para 2 of the Article 8.Therefore, the Court had to determine whether the Respondent (State) complied with its oblkigation not to interfere with the Applicant's right to respect for her private life, and if so, whether that interference satisfied the conditions laid down in the second paragraph of Article 8: was it 'in accordance with the law'[73].

Regarding whether there has been an interference, the Court reiterates that the concept of private life includes elements releting to a person's right to their image and that the publication of a photograph falls within the scope of private life[74]. The

[72] **Judgement for the case of Sciacca V Italy**, at P.6
[73] **Ibid**, at P.7
[74] *See* the Case of **Von Hannover V Germany** [No. 59320/00, ECHR 2004-VI

Court concludes that there has been an interference[75].The Court further concludes that the intereference itself has not been shown to be in accordance with the law[76]. That finding is suffient for the Court to conlude that there has been a breach of Article 8 stated above.Accordingly, it is note necessary to determine whether the interference in question pursued a legitimate aim or was necessary in a democratic society to achieve that aim[77].

Conclusively, form the discussions above and by the support of the historical development of Data protection in various parts of the world and the urge of various Countries at the individual level and later the joining of force of such Countries on responding to the challenges posed by the growing activities of infringement of private life, it prompted the enactment of various Convention on adressing for the same and even enforcement of such Conventions as observed in Sciacca case.

3.2 The Concept of Data Protection

3.2.1 The Scope of Data Protection

The application of the Data protection legislation or any measure to do so, have to be evolve on certain parameters on knowing who play what role as far as Data Management is concerned. To start, is by looking on the **Personal Data** is defined by the Data protection Directive[78] to mean;

> " any information relating to an identifiable natural person (data subject)"[79].

[75] **Supra note 74**, at P.8
[76] **Ibid**
[77] *Also see* the case of **M. v the Netherlands** [No.39339/97
[78] **Directive 95/46/EC**
[79] **Article 2 (a)**, Ibid

The same Article has gone a mile stone on describing the other terms on the same on definition and stating that;

> *"an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*[80].

Although in its early stages data protection law tended to apply almost exclusively to textual information, developments in technology mean that almost any form of recorded information is likely to come within the ambit of the legislation.In the event that an individual interacts with an automated telephone service by speaking a series of numbers or words to allow a call to be directed to the appropriate department, those recorded words will class as personal data[81]. Further, another category of personal Data may be the Biometric Data.Here in Tanzania for example, the the taking of Biometric Data from the Applicant of National Identity Card during the registration and identification of persons would inlude the taking of the digital picture of a person and the fingerprints.This again satisfies the clarification of the discussions above.As stated in the defition above, a photograph of an individual and te fingerprints are indeed the peace of information and again they do belong to an identifiable person.

The word 'any information' has been given a wider analysis by the Opinion of the Working Party[82] which they went a milestone by stating that;

---

[80] **Ibid**
[81] Lloyd, J., I., **Supra Note 59**, at P.40
[82] Under **Article 29** of the **Data Protection Directive**

"From the point of view of the nature of the information, the concept of personal data includes any sort of statements about a person. It covers "objective" information, such as the presence of a certain substance in one's blood. It also includes "subjective" information, opinions or assessments. This latter sort of statements make up a considerable share of personal data processing in sectors such as banking, for the assessment of the reliability of borrowers ("Titius is a reliable borrower"), in insurance ("Titius is not expected to die soon") or in employment ("Titius is a good worker and merits promotion")"[83].

Sensitive Data is another important area to understand in the scope of application of personal Data.The Data Protection Directive (95/46/EC1) and the Council of Europe Data ProtectionConvention of 1981 are based on the premise that certain categories of personal data, asdistinct from all other personal data, require extra protection and may be processed by privateand public bodies only for specific purposes and under special conditions[84].

The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "normal" personal data. Misuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment. For this reason, the Convention and the Directive make the

[83] Available at **<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>**
[84] Article 29 Data protection Working Party**, "Advice Paper on special categories of Data",** at P.2

processing of data which by their nature are regarded sensitive dependent on certain safeguards and conditions, which go beyond the conditions for the processing of other personal data[85].

This can well be elaborated by the rulling in the case of **Regina v Chief Constable ex parte AB[86],** where it was held that;

> *"As a general rule of good public administration, the police should not disclose information acquired in the course of performing their public duties, in relation to a member of the public, which was not generally available and was potentially damaging to that person if disclosed. However where the police considered in the exercise of a careful and bone fide judgment that it was desirable or necessary in the public interest to make disclosure for the purpose of preventing crime or alerting members of the public to an apprehended danger, they were entitled to make such limited disclosure as was judged necessary to achieve that purpose"*[87].

Conclusively it can be obseved that, certain disclosures of this special category of Data is permissible only if the Law has permitted or on the legitimate ground for the good of the Public in the sense that, it non disclosure may lead to the harm of the public and again its disclosure may not harm the individual in possession of such data. This is vivid when the European Court of Justice was asked to rule on the question of whether the reference to the foot injury of Mrs Lindqvist's colleague constituted sensitive data relating to health.The Court ruled that;

---

[85] **Supra Note 84.** *Also see* the case of **Campbell V MGN Ltd**
[86] [1999] QB 396
[87] *See* the case of **Cole V. States of Jersey Police**.[2007] jrc 240

> *" In the light of the purpose of the Directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual"*[88].

Another key area to venture is term **relating to the Data Subject.** The motive here is find an answer as how to establish the relationship between a certain individual with the certain Data.Neither the Directive nor the Act provides any definition when data relates to an individual and this has been a rather contentious issue[89]. This scenario can well be captured in the case of **Durant v Financial Services Authority**[90] where the Court was caught on the situation where it had to establish as to whether the information required by the Appelant was connected to him or not. It revolve on the premise that the personal Data of an individual must be connected to the individual for it to be said that it has been violated.it has also given an exception to that to the effect that not always when the information is connected to the individual is published must amount to the infringement of such information.In the case of **Common Services agency v Scottish Information Commissioner**[91], Lord President ruled as follows;

Although the undelying information concerns important biographical events of the children involved, by the stage of the compilation of the barnardised table that information has become not only statistical but perturbed to minimise the risk of

[88] *See* the Case of **Bodil Lindqvist.** Case 101/01, [2004] QB 1014
[89] Lloyd, J., I., **Supra Note 59**, at P.43
[90] [2003] EWCA Civ 1746
[91] [2008] UKHL 47

identification of any individual child.It is no longer, in respect of any child, 'biographical in a significant sense'. The focus has, in my view, also moved away from the individual children to the incidence of disease in particular wards in particular years. The rights of privacy of the individual children are not infringed by the disclosure of the barnardised data"[92].

Conclusively,The Court in ***Durant case*** (supra), the Court stated that the Data only relates to a person only when that Data that relates to a person is information that affects the privacy, whether in his person or family life, business or professional capacity.To assist the Court suggested two criteria for assessment; first is whether the Data is biographical in nature,i.e how far it is concerned with person's private life, and second,its focus, whether on the person, or someone else or something else[93].

Further, the **concept of processing** is another area to understand in the broad concept of the Data protection regime.Data may be processed for various purposes by various parties. If these processes may not be regulated, then the infringement of the Data involved in the process is likely to occur and cause harm to the Data subject to whom such Data is related at that material time. The Data processing systems and its meaning, can be grasped from the The Directive[94] for the Data protection, of which in this Chapter, this Directive and the European Union Data protectiion

[92] *Also see* the Case of **Durant v Financial Services Authority.** [2003] EWCA Civ 1746 where the Court also ruled that the 'mere mention of the data subject in a document held by a data controller does not necessarily amount to personal data'.
[93] Ibid
[94] **Directive 95/46/EC**

perspective is chosen as a classical study case to be used.This Directive has provided the following;

> *"processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"*[95].

The definition has tried to cover many aspects so as to include them as part of Data processing in order to avoid any ambiguity and not to leave certain acts being regarded as not processing. This can be justified for example by the word 'storage'.From the normal thinking, is hard to convince a lay man that, if the latter has just stored an information of a person, he has considered to have processed it.However, the Directive has also pointed out that even 'storage' of Data amounts to the processing of such Data.

Other Literatures[96] has defined Data processing as;

> *"the collection and manipulation of items of data to produce meaningful information"*[97].

Conclusively, although all forms of processing are potentially covered by the Data Protection Directive, the most stringent controls apply in the case of processing by

---

[95] *See* **Article 2(b)** of Directive 95/46/EC
[96] Carl, F., (1996), **"Data Processing and Information Technology"** (10th ed.). Thomson,ISBN 1844801004, at P.2
[97] *Also* available at **http://en.wikipedia.org/wiki/Data_processing**

automatic means. It is arguable that any use of a computer to create a document comes within the scope of this criterion, as there is no direct physical link between the Author pressing a key and a letter or symbol appearing on the screen.The act of loading a page onto a web server involved a number of operations, some at least of which are performed automatically[98].

3.2.2 The Data Protection Actors

There are key stake holders through whom personal data revolve around.As stated earlier, before embarking on proposing the data protection regime here in Tanzania, it is of paramouncy importance that all key concepts related to the Data protection Regime are well understood and captured. The Actors in the Data protection are of significance to be known and the role of each one.These Actors are Data Subjects, Data Processors and Data Controllers.

Starting with the **Data Subject.** Various sources define differently on who the Data Subject is depending on the context on which the Composer has chosen.The Encyclopidia defines the Data Subject to mean;

> "data subject An individual about whom information is stored in a computer-based system"[99].

On the other side, the United Kingdom Data Protection Act[100] has defined the Data subject quite differently from the other plain definitions to mean;

> *" an individual who is the subject of personal Data"*[101].

---

[98] Lloyd, J., I., **Supra Note 59**, at P.51
[99] *Also* available at **http://www.encyclopedia.com/doc/1O11-datasubject.html**
[100] This Act is the precursor of the UK Data Protection of 1984.

In a simple understanding, the Data subject is a person who possesses the particular Data and at same time that particular data relates to him.This would therefore entitle that person a right to search for correctness of various details concerning his Data[102].

Data Controller is another actor in the Data protection Regime.Again the various authorities have attempted to describe as to who the Data Controller. Most of them being the Legislative Instruments.Starting with the Data protection Directive which defines Controller as follows;

> *"controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law"*[103].

Further, the United Kingdom Data Protection Act of 1998 on its side has defined Data Controller to be regarded so when it;

> *"subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed"*[104].

However, as regarding the Data Controllers in for example electronic mail or telecommunications, the Directive on data Protection has elaborated more on data

---

[101] Under **S.1 (1)** of the UK Data Protection Act.
[102] *See* Lloyd, J. I., **Supra Note 59**, at P.56
[103] **Article 2(d)** of Direcive 95/46/EC
[104] **S.1(1)** of the UK **Data Protection Act**

Controllers to the following effect;

> *"Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service"*[105].

This position was also made clear in the case of **Data Protection Registrar V Griffin**[106] where it was confirmed that anyone who processed data on behalf of clients would be regarded as a Data user(now Controller) when he or she possessed any control or discretion concerning the manner in which the processing was carried out[107].

Data Processor is another actor in the Data protection regime.The Data Protection Directive and the United Kingdom Data Protection Act act as Model Laws for purposes of this Dissertation as stated earlier in the beggining of this Chapter, has given the following meaning to Data Processor as follows;

> "processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"[108]

---

[105] **Recital 47** of Directive 95/46/EC
[106] *The Times*, 5 March, 1993
[107] *See* Lloyd I.J. ,**Supra Note 59,** at P.55
[108] Under **Article 2(e)**

On its side, the Data Protection Act (supra), has defined the Data Processor as;

> "..Any person(other than an employee of the data controller) who processes the data on behalf of the data controller"[109].

It is upon the Controller to ensure that the security on the Data possessed is satisfactory and even making sure that he select the appropriate Data Processor whom would not make any abuse of personal Data availbale to the data Controller.This agaain proves that the Data processor performs his or her functions on behalf and under the instructions of the Data Controller[110].

Another key issue to understand is that, the relationship between the Data Processor and the Data Controller is contractual and has to be done under the written agreement between the two Parties.A written Contract must also be entered into obliging the processor to act only on instructions from the controller in respect of the processing carried out, and also to comply with the requirements of the seventh pricnciple[111].Further, it is only the Data Controller who may be liable to compensate data subjects for losses arising from processing[112].

Therfore, within the umbrella of the data protection Regime, there are Key actors whom are inevitable in various processes concerning the Data protection. There are those processing, some Controlling and others to whom such same Data relates.

---

[109] Under **S.1(1)** United Kingdom Data Protection Act.
[110] *See* Lloyd,I.,J., **Supra Note 59**, at P.56
[111] **Schedule 1,Pt 2, para. 12** of the UK Data Protection Act of 1998
[112] **S.13** of the United Kingdom Data Protection Act.

3.2.3 The Data Protection Principles

The Data protection Regime in its operation is dominated by a number of principles which are main tenets on how should Data should be processed.All these initiatives forms part of the grand plan of making sure that the Data belonginng to a certain individual is not easily abused and there must be certain standards to be observed which would eventualy being used as a measure on how Data has to be treated.

Again, these principles never emerged just within short period of time.But it took some times for them to revolutionise after caefuly coining done by experts who considered various circumstances before. As declared earlier, the model which will be used is the European Union Directive on Data Protection and the United Kingdom Data Protection Act.The European Union on their side has done quite an intensive research of this area of study.The Data protection Directive[113], describes the following as being the principles that Member States Member States shall oberve and at the same time making sure that personal data must be;

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

[113] Under **Article 6**

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The Directive has further provided that It shall be for the Controller to ensure that paragraph 1 above is complied with[114]. Here the Directive is emphasising that this duty is such duty to be obeserved by the Data Controller whomhave been thoroughly elaborated in the preceding part 4.2.2 of this Chapter,above.

On its side, the Data Protection Act has provided many principles than the Directive for Data Protection which are to be used on processing Data. Such principles are as follows[115];

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless–
    (a) At least one of the conditions in Schedule 2 is met, and
    (b) In the case of sensitive personal data , at least one of the conditions in Schedule 3 is also met.

[114] Under **Article 6(2)**, Ibid
[115] These Principles are provided for **under S.4** and enlisted in the 1st Schedule of Part I of the same Act.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act .
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data .
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For the more clarity, this Chapter will cover the Data protection principles covered by the Directive for Data Protection and elaborate them one by one by giving examples. Starting with the fair and lawfully processing of data.the processing of Data must not just be from the the will or discretion of the Data Controller but must have the backup of the law.And further, this process must observe degree of fairness

and not just an abrupt processing which does not consider any element of civilisation and the welfare of an individual.

The Data protection Directive has further provide for the criteira which must be observed before the Data is processed.In this area therefore, data cannot be processed unless;

a) The data subject has unambiguously given his consent; or
b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) Processing is necessary in order to protect the vital interests of the data subject; or
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)[116].

[116] **Article 7** of the Data Protection Directive.

One of the good case which may satisfy both the requirements of Article 6[117] regarding principles of Data Protection and Article 7[118] regarding the Criteria for the processing of personal Data is the case of **David Paul Johnson .V. The Medical Defence Union Limited**[119]**,** where the Claimant Mr. Johnson claimed before the Honourable High Court of Justice,Chancery Division that his personal Data was unfairly processed with intention to termainate him.

Conclusively,The Data protection principles span the whole continuum of data processing, from the stage when the Data is first acquired, perhaps using pen and paper, to the time when it is permanently and irretrievably destroyed. A formula frequently used to justify data protection legislation is to the effect that there should be no processing whose very existence is a secret. More expansively, the principles seek to ensure that dat subjects are aware who processes data about them and for what purposes; they should feel confident that it would be kept in secure conditions and that they will be able to verify the accuracy and relevance of the Data held[120].

[117] Of **Directive 95/46/EC**
[118] **Ibid**
[119]**2006] EWHC 321 (Ch)**
[120] Lloyd, **op.cit**, at P.87

CHAPTER FOUR

4.0 FINDINGS AND ANALYSIS OF LEGAL FRAMEWORK FOR DATA AND PRIVACY PROTECTION OF TANZANIA: LACUNA AND CHALLENGES OF ITS ABSENCE

This Chapter focuses on examining and analysing the findings on various Lacuna oberved in the current Legal Framework Regime on Data Protection and Privacy in Tanzania and how it is provided for by various provisions of scattered Legislations in Tanzania, though not in a single Legislation.Each Legislation and its particular provisions dealing with Data protection will be analysed.

Further, in the other part of this Chapter, it will elaborate on the significance of the presence of the Data protection Legal Framework in the United Republic of Tanzania at large and for the benefit of the now existing National Identification system, in particular.

4.1 Analysis of Lacuna in the Current Legal Framework for Data Protection and Privacy in Tanzania

To date, the Tanzania has no a one compounded piece of Legislation which is providing for the Data protection and privacy matters in Tanzania.The Parliament of Tanzania has not so far enacted this kind of Legislation.

4.1.1 The Constitution of the United Republic of Tanzania

The Constitution of of the United Republic of Tanzania (hereinafter, 'The Constitution'),which is currently in force, is that of 1977 and has been amended on

various occassion. This is the Supreme Law of the Land in Tanzania and all laws in force are inevetably have to be in comformity with it,short to that, such other Law is rendered Null and Void[121].

On its side, the Constitution[122] has provided for the Right to privacy and recognising the Consitutionality of that right in Tanzania. On this, it provides 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"*[123].

However, the same Constitution has not granted this right with absoluteness, but it has subjected it to certain bureacracies of the Government during such processes of granting it. Here, the Constitution further 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"*[124].

---

[121] *See* the case of **Kukutia Ole Pumbun and Another v. Attorney General and Another [**Civil Appeal No. 32 of 1992]
In this Case, the Court of Appeal of Tanzania, held *inter alia*, that certain provisions of the Government Proceedings denied the Appellant of his Constitutional right of Accessing justice form the Court of Law by requiring him to first obtain Consent of the Minister to be able to sue the Republic, and therefore declared **S.6** of **Government Proceedings Act** of 1967 as amended by Act No.40 of 1974, as Unconstitutional.
[122] of the United Republic of Tanzania of 1977 as amended.
[123] **Article 16(1)**, Ibid.
[124] **Article 16(2),** *supra note 102.*

If you look at the **Sub-Article 2 of Article 16** of the Constitution, you can see that the right to privacy which has been provided substantively, its grant may be put into jeopardy buy the technicalities which may put brought up by the procedures which are set and said to be the once to provide on how that right to privacy may granted.

The Second instance where the Constitution bars the absolute enjoyment of the right to privacy is thorugh maintaining the provisions of **Article 30(2)**[125] which provides that;

> *"It is hereby declared that the provisions contained in this Part of thisConstitution 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.....*"

Regarding **Article 30(2),** of the Constitution, the Hight Court of the United Republic of Tanzania once held that;

> "A law which seeks to limit or derogate from the basic right of an individual on the grounds of public interest, will be saved by Article 30(2) of the Constitution, if it satisfies two requirements: firstly, such law must be lawful in the sense that it is not arbitrary. That means it should make adequate safeguards against arbitrary decisions and provide effective controls against abuse of those in authority when using the law. Secondly, the limitation imposed by such a law must not be more than is necessary to achieve the

[125]This Sub-Article has provided may Instances where the Human and other provided can be denied for various reasons provided therein from **para (a)-(f)**

legitimate object. This is also known as the principle of proportionality"[126].

Conclusively, one may say that, though the right to privacy has been thoroughly stated in the Supreme law of the Land, the many limitations imposed in unto its absoluteness and its enjoyment may render it non-existant to the judgement that it has not been provided for within the Constitution or its is better for it not to appear there under the auspices of **Article 16** of the same Constitution.

4.1.2 The Electronic and Postal Communication Act of Tanzania (EPOCA)-Act No.3 of 2010

The Electronic and Postal Communication Act (Hereinafter EPOCA for purposes of this Dissertation) is an Act of Parliament of the United Republic of Tanzania which was enacted to harmonise the postal and communications regualtion in the Country. EPOCA was passed by the Tanzanian Parliament on January 29, 2010 and assented to by the President on March 20, 2010. The Act came into force on May 7, 2010.14 It repealed and replaced two pieces of legislation in the Tanzanian communication sector: the Broadcasting Services Act and the Tanzania Communications Act.It also amended the Tanzania Communications Regulatory Authority Act and the Fair Competition Act.However, it saved all regulations made under the repealed laws to the extent that they are not inconsistent with EPOCA and not expressly revoked[127].

---

[126] See the for example various cases of **Kukutia Ole Pumbun v Attorney General** [1993] T.L.R. 159; **Julius Ishengoma Francis Ndyanabo v Attorney General ,** Civil Appeal No.64 of 2001, Court of Appeal of Tanzania, at Dar es Salaam (Unreported); **Legal and Human Rights Centre v Attorney General**, Miscellaneous Civil Cause No.77 of 2005, High Court of Tanzania, at Dar es Salaam (Unreported); **Christopher Mtikila v Attorney General**, Miscellaneous Cause No.10 of 2005, High Court of Tanzania, at Dar es Salaam (Unreported).

[127] Makulilo, B.A., (2011), **"Registration of SIM cards in Tanzania: a critical evaluation of the Electronic and Postal Communications Act 2010"**, *Computer and Telecommunications Law Review*, at P.3

EPOCA was enacted with three fundamental objectives.The first was to address the challenges posed by modern technologies, especially the convergence of technologies. The second was to harmonise and consolidate communication laws in order to overcome regular conflicts in their implementation, and the third was to introduce the Central Equipment Identification Register (CEIR) and registration of SIM cards[128].

On the part of the protection of Data and even privacy of the Data subjects subscribing themselves with the various Mobile Companies, the Act requires that every mobile phone owner to register his o rher Sim Card with the respective Company which he previously subscribed him or herself with. This requirement is provided for by EPOCA by stating that;

> *"Every person who owns or intends to use detachable SIM card or built-in SIM card mobile telephone shall be obliged to register SIM card or built in SIM card mobile telephone"*[129].

During registration, an Applicant is required, apart from filling the registration form provided by the respective Company, to supply the following attahment bearing his or her particulars. the full name of the potential subscriber;identity card number or any other document which proves identity of the potential subscriber; and residential and business or registered physical address, whichever is applicable[130]. The element of confidentiality to be maintained by the subscribing Company regarding the

[128] Makulilo, B.A., (2011), Supra Note 127, at P.3
[129] *See* **S.93(1)** of the Electronic and Postal Communication Act of Tanzania [Act No.3 of 2010]
[130] *See* **S.93(2) (a),** Ibid

information obtained during registration is clearly imposed.EPOCA requires the subscribing Company to treat the information obtained during registration of the Sim Card as confidential.EPOCA has clearly stated this position by stating that;

> *"A person who is member, employee of applicationservice licensee, or its agent, shall have a duty of confidentiality of any information received in accordance with the provisions of this Act"*[131].

Again the EPOCA further states that;

> *"No person shall disclose the content of information of any customer received in accordance with the provisions of this Act, except where such person is authorised by any other written law"*[132].

The concern however comes up due to the fact that, the excercise of this right which favours for the Data protection is again subjected to the procedurall requirements similar to that of **Article 16(2)** of the Constitution of the United Republic of Tanzania of 1977 as amended. It empowers certain Agencies to ask from the Phone Companies for certain informations which they find fit for the improvement of security issues.But not only does the Act provides for that,it has also provided some other circumstances which it find suitable to allow the information of a person to be revealed.It provides that;

> "A person shall not disclose any information received or obtained in exercising his powers or performing his duties in terms of this Act except -

[131] *See* **Supra Note 129**, S.98(1)
[132] *See* **Ibid**,**S.98(2),**

(a) Where the information is required by any law enforcement agency, court of law or 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 authorised 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"[133].

Conclusively, if this privellege of disclosing such information given to the certain categories of person as stated above is abused, then Data of that particular individual which has been obtained may may fall into wrong hands maybe due the influences of corruption or element of unfaithfulness on the part of an Employee of the registering Company.

4.1.3 The Registration and Identification of Persons Act (RIPA) of Tanzania

This is the main Legislation providing for the main issues regarding registration and identification of all eligible persons in Tanzania.The Registration and Identification of persons Act (Hereinafter RIPA for the purposes of this Dissertation) was enacted by the Parliament of Tanzania as Act No.11 of 1986 and assented to by the President

[133] **S.99** of Act No.3 of 2010.

on the 6th of January, 1987.But it was never enforced until 2011 by **Government Notice No.257A** which was published on 26th August, 2011.The Gazzette[134] pointed out 1st day of September,2011 as the day which Registration and Identification of Persons Act should come into operation.

The Long gap between enactment and enforcement of the Act which was withheld for the period of over 26 years, was due to the number of overridng factors.The main reason was that the Government could no longer pursue with the implementation of the National Identification Project due severe lack of fund and the economic challenges that the Government used to face by then.It is a known fact that the Governement was just from the ashes of war it fought with Uganda to overthrew Dictator Iddi Amin and the massive inflation of early 1980's.This was more empahised by the Government as follows;

> *"It was appreciated though by all concerned that the Government was not in a position to carry out this excercise given the huge cost involved. By then the Country was at the lowest ebb of economic decline which began in the late 70s. The decline was exacerbated by floods and cholera outbreak (1977), war with Dictator Iddi Amin's invading forces (1978/79), prolonged drought(1981-1984) and the donor fatigue"*[135].

Regarding Data protection and the matters relating to privacy, RIPA does impose an obligation on the part of a Registration Officer or any other Officer performing a

---

[134] **No.34 Vol 92** dated 26th August,2011

[135] Gotham International Ltd (2006), **"The Feasibility Study Report on National Identification and Registration of persons program for the Government of the United Republic of Tanzania**", at P.48

duty on implementing RIPA not to disclose any information gathered in the course of his employment and failure to do so may invite some jail terms.On this RIPA provides that;

> "Subject to section 18, the Registrar and any registration officer and any immigration officer performing functions under this Act shall not-
>
> (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"[136].

However, it allows the Minister to permit such disclosure upon certain reaons and with certain conditions set therein.Here, RIPA further provides that;

> "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"[137].

As observed, the Act has not imposed sanctions and other restrictions on the part of other Data Actors inluding the the Data Processors or the Data Controller just in case this Personal information happens to fall on the hands of other entities appart from the National Identification Authority (NIDA) of Tanzania during interfacing.

---

[136] *See* **S.19** of the **Registration and Identification of Persons Act**. (Act No.11 of 1986)
[137] **Ibid.**

4.1.4 The Records and Archives Management Act of Tanzania

The Records and Archives Management Act (hereinafter the Act for the purposes of this part of the Disseration), is the creature of the Parliament of the United Republic of Tanzania enacted in the year 2002 and is the Act No.3.It was assented by the then President of Tanzania, President Benjamin William Mkapa on 28th March,2002[138].

In its long title, the Act has stated the purpose of its enactment to the following effect;

> *"An Act to establish the Records and Archives Management Department to provide for the proper administration and better management of public records and archives throughout their life cycle, to repeal the Records (Disposal) Ordinance,1931, and the National Archives Act, 1965, and for connected matters"*[139].

Just from the explanation of the Long title of the Records and Archives Management Act as stated above, it is undoubtful that, amongst the information which would be managent by the said Department created,would include the personal information of individuals whom by the virtue of their employment or any other reason which justified such collection,made them the subject of such records. For purposes of clarity, the key terminology connected with the substance of this Dissertation, has to be defined as according to the definition given by the Act as follows;

Record to mean;

---

[138] Also available at **http://bunge.parliament.go.tz/PAMS/docs/3-2002.pdf**. Visited on 28th July,2013

[139] *See* **the Long title of the Act No.3 of 2002** of Tanzania

"recorded information regardless of form or medium created, received and maintained by any institution or individual in thepursuance of its legal obligations or in the transaction of its business And providing evidence of the performance of those obligations or that business"[140].

Public Record as;

"the records specified in the Schedule to this Act"[141].

Private Record as;

"means records other than public records specified in the Schedule to this Act"[142].

Archives as;

"means records of enduring value selected for permanent preservation"[143].

Now, of interest regarding issues of Data Protection and privacy issue revolves within the provision of **S.16**[144] regarding the so called 'Thirty (30) years rule'which allows for the Records or Archives to be destroyed after they attain the period of thirty years since they were created.The Act reads as follows;

"Subject to any written law prohibiting or limiting the disclosureof information any public record, public records in the NationalArchives, in any other archival repository under the control of the Directoror in a place of

[140] *See* **S.2**, Ibid.
[141] **Ibid**
[142] **Supra Note 139,** S.2
[143] **Ibid**
[144] **Ibid**

deposit appointed under section 15 of this Act, shall be available for public inspection after the expiration of a period of thirty years from their creation, calculated as prescribed in subsection (2) of section 4 of this Act, except in so far as a longer or shorter period may have been prescribed by the Minister by regulations made in accordance with section 28 of this Act at the request of the head of the public' office which created the records or its successor in function"[145].

The Act further provides that;

"A longer period than thirty years may be prescribed under subsection (1) only when there is a continuing need to restrict public access on grounds of -

(a) National Security;

(b) Maintenance of Public Order;

(c) Safeguarding the Revenue; or

(d) Protection of the Privacy of living Individuals"[146].

Now analysing the two Subsections above, yes it is a good approach to allow the access by the Public of the said Documents after such a long time of retention, and again restricting the same access to some other Document by prolonging the time of thirty (30) to more as the Minister may stipultate[147] in the Government Gazzette.
But issues relating to Data and Privacy Protection,it would be sounding for the sake of protection of personal Data, for it to be provided in the same Act that personal

[145] Under **S.16(1)** of Act No.3 of 2002 of Tanzania
[146] *See* **S.16(3)** Ibid
[147] *See* for the Powers of the Minister regarding duration of Records and Archives retention as provided by **S.16(1),** Ibid

data are not subject for public sctrutiny not just by elongating the time from thirty (30) years to more years, but by exempting completely personal Data and sujecting them to other Legal Mechanism of Data Protection principles on the processing of Personal Data, and not simply by saying now this personal Data can go Public.This is due to the fact that personal data is personal Data regardless how they were obtained. Therefore, this is another piece of Legislation which has tried to set up some intiatives[148] on protecting personal Data and the privacy of the individuals but there should be set principles of world standard on how Data concernig private life of an individual can be protected. They not be subjected to thirty (30) years Rule only, but to a special category of Information and its own mechanisms on how to handle them.

Conclusively, after the analysis of some of the Legislations that attempted to protect personal Data and privacy issues at large, it is now a proven case that Tanzania has no a single piece of Legisltion within which all matters of Data Protection and Privacy are comrehensively being provided for. But these attempts have been made on the scattered pieces of legislation for various purposes.

As seen above, most of the Legislation denies the disclosure of certain personal Data but on the other hand allows such disclosure by only observing the permission of the Minister responsible in that Ministry but without mentioning of the prior consent of the data Subject whose Consent is paramount under the Pricinciple of Data protection regard the processing of personal Data.

[148] *Also See* **S.16 (3) (d)** of Act No.3 of 2002.

4.2 The Challenges of Absence of Data Protection and Privacy Legal Framework and the Significance of its Presence in the National Identification System

As observed from the previous Chapters, the emergence of National Identification system in the various parts of the world has resulted into the extraction of huge amount of personal information from the the people resident in the respective Countries.The application for one to be included in the National Identification system is the mandatory as these people are required to do so by the law and not by their will.A good example of such establishment by the statute regarding Registration and Identification of persons here in Tanzania, is the presence of the Registration and Identification of persons Act of 1986.All current registration and Identification of persons here in Tanzania form 2012 to date is executed under the mandate provided so by this Legislation.

These Data once collected and the issuance of the Identity Card is done, the next thing one has to consider is the administration and processing of such massive amount of Data collected during their use, extration, access to such Data and the ultimate destruction of the same personal Data previously collected. For the case of Tanzania for example, as it has been stated in the Feasibility study[149] that, after the execution of registration and identification of persons and the Data already collected, then they may be used for various purposes apart from only used to issue one the Identity Card.

[149] Gotham Internaional Ltd (2006), "**The Feasibility Study Report on National Identification and Registration of persons program for the Government of the United Republic of Tanzania"**, at P.104

It was stated that;

> *" The National ID system is part of a larger vision that will further enable integration with other nationwide governmental and administration systems as well as be the starting point for secure access and usage of forthcoming e-Government services in Tanzania.It is also open for controlled access and usage by private businesses allowing using the high level of trust provided by the program also for increasing the security of transactions between Citizens and Businesses"*[150].

If clearly obeserved, the once the National Identification system is complete here in Tanzania in a full fledge scale, then the massive individual Data collected during the registration and identification of persons would be shared with other stake holders through interfacing mechanism as experience form other Countries with the already established syastem does so.

A good example is the Kenya National Registration Bureau. When we paid a visit to its Head Quarters in Nairobi in august 2011, we were informed that the many request were made by various stakeholders some being the Governement Department like Criminal Investigation Department, Police and Social Security Funds not forgetting the Ministry of Finance. The other group making querries are private business entities like the Insurance Companies, Banks and Securities Companies. All these entities whether Governmet or Private, simply request for personal data regarding their Client for various reasons some being for authentication and examination of genuiness of certain pieces of Information.

[150] Gotham Internaional Ltd (2006), **op.cit**, at P.104

With this kind of practice therefore, though these stakeholders are given information under certain strict conditions and under legal obligation of not disclosing such information during the conduct of their businesses, there is a need of these Sxtakeholders of having know-abouts of the Data Protection Principles[151] so as to properly hanlde such personal data of which some are sensitive. Once there is a firm Legal framework providing for such protection, automatically, during interfacing, the Key Data Players being Data Controller, Data Subject and the Data Processor each would know his rights and obligations and therefore a complete avoidance of abuse of such personal Data given to them by the National Identification Authority (NIDA). This example may be sufficient to explain. We expect after proper establishment of the National Identification systems, Banks as one of the Private Stakeholders to interface with NIDA in order for them to identify certain individuals who apply for loans from the Bank.

The trouble from the above scenario may arise this way, the Bank after receiving this information may not end up using it for purposes of processing the Loan, it may end up using it for other purposes beyond those stated to NIDA as a reason for them to be given such information. But if the law regarding processing of Data is properly resonates within the knowledge of the Bank and the consequences of not abiding by the principles of Data processing, the latter will hesitate to use such Data for any purpose other than that for which they requested that information for.

Because, through few weak mechanisms of implementing interfacing, for example through data Sharing Agreement or Memorandum of Understanding or other means

[151] *See* for example **Article 6** of European Union Directive on Data Protection (Directive 95/46/EC)

so decided, one would not be in a good position to tell his role in the whole cycle of Data and Privacy protection.So, one knows that I am a Data Controller,Data Processor, Data Subject and the role and obligation of each one is provided in the Data Protection Act,if existent for example, one would be in a position to make reference to satify him or herself regarding measures he should take to protect such Data provided to him during interfacing.

Further, in the presence of Data and Privacy protection Legal Framework Regime, it will have a positive impact to the reactions of individuals whom are required to provide for their information.The Data Subjects here would not worry of the abuse of their personal information which they have provided to the Data Controller. Moreover, the presence of the Legal framework for Data and Privacy Protection will boost the urge of Westerners in the participation in the National Identification project as they would know that the requirements of **Article 25**[152] of the European Union on the Transfer of personal data to the third party Contries has been satisfied.This provision provides that;

> *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection"*[153].

So putting into place of a firm Legal Framework for Data Protection and Privacy

[152] Of Directive **95/46/EC of the European Union on Data Protection and Privacy**.
[153] **Ibid**

would simply the entire work of Data processing after the system is well established and devoid National Identification Authority of Tanzania (NIDA) of a burden of reminding its Stakeholders of the duty of fair and lawful processing of such Data given to them by NIDA during interfacing.

Conclusively, Data Subjects whom are registered with National Identification Authority may well be protected by NIDA under the duty of non-disclosure of the such personal information gathered during registration before this information leaves NIDA through interfacing, but are not well covered if NIDA will start interface with other Satakeholders whom will request such information for various purposes in the transactions.With the enactment of Data Protection Act, the Data Subjects will be much secured.

CHAPTER FIVE

5.0 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Circumstances emerging on various occasions in the human History has been a source of many challenges in the Human lifes and consequently prompting certain actions including legislative actions to harmonise such situations and restore harmony and well being in the daily conduct of life of the people. And again, an initiative to tackle the one challenge observed may leave the other unseen challenge ahead which may be created by the indirect impact of the first undertaking which was designed to tackle the first challenge.

This notion can be explained by the urge by various Countries to be able to identify their people for various reasons as explained in the preceding Chapters. Some decided to do so due to the aftermath of the terrorist attack so to be able to track criminals and their networks, some introduced National Identification system a platform for future introduction of e-Governance, some to improve integration of various systems of the Government amongst themselves and between the Government system and the private systems.

All these initiatives and the urge to implement the National Identification system meant to correct such mischiefs as stated above, has brought up another challenge which now has to be tackled after the establishment of the National Identification system.Before it was the need for the firm National Identification system capable of identifying every one residing in that particular jurisdiction.A successful implementation and installment of this system, create a new challenge of having a

system which would ensure the smooth running of the existing system.

Now, the consequent system required for the smooth running of the previously established system of National Identification is the establishment of the Legal framework for Data and privacy protection.Once the massive personal Data are collected for the purpose of issuance of the Identity Card,, and later for the other purpose of sharing with the stake holders for their own business use, then the priciples of Data Protection are inevitable. What is actualy created are typically different Actors of Data Processing similar to those in the Data and Privact protection regime, being the Data Controller, Data Subject and the Data Processor.Again, how these Actors conduct their activities by using the personal data in their custody are strictly guided by the Data protection principles.

If National Identification Authority collects Data form various persons through mandatory registration and identification, automaticaly the acquire the position of being the Data Controller and later provide some information through interfacing with other Institution which later they will become Data processor. Sometimes situations arise which would make Data to be required for certain reasons. In these situations, is when the vitality of Data protection Principles comes in. This phenomenon can be illustrated by the event of September 11th, 2001where intervention on electronic communications were inevitable as to be able to know what Terrorist were planning next. One of Institutions affected were the Communications companies[154].

[154] *See* Lloyd, J.I., **Supra Note 59**, at P.18

Then, it is these legislative powers conferred upon Security Organs to access personal Data which now invite the application of Principles of Data Protection. The law[155] requires that, though the intervention of such data is on good faith, the processing of any personal Data must abide by the principles of Data protection.

On her side, **Liu, Y.N** in her Article[156], has elaborated on the efficiency of the Data protection in the National Identification systems. She argues that, if Data, whether Biometric or any leads to the identification of a person, then automatically it has falls under the auspices of Data protections constraints. Here she argues;

> *"It has been argued that when biometric information is used for verification, stored in an offline situation, for example: smart card, or local database, and without any additional identifiable information such as names, or addresses, it can be regarded as truly anonymous. Therefore it is safe to exclude it from the constraint set by the data protection legislation"*[157].

The idea here is that, if the Biometric Data can hide the key particular of an individual, for example the Name or any ethnic details, then it will succeed to create anonymity regarding that person. In this kind of a situation, such Data is not subjected to any Data protection priciples.

In the absence of the Data Protection Legal regime, once the Data are interfaced to untrust worthy Institutions,despite the presence of Data Sharing Agreement or Memorandumm of Understanding between them, the likelyhood of the abuse of such

---

[155] *See* **Article 6** of Directive 95/46/EC. *Also* **Schedule 1** of United Kingdom Data Protection Act

[156] Liu, Y., N., (2008), **"Identifying Legal concerns in the Biometric Context"**, *Journal of International Commercial Law and Technology*, Vol.3, Issue 1, pp 45-54

[157] *See*, **Ibid**, at P.48

Data may occur which may be injurious both to the Data Controller and the Data Subject.

Therefore,the idea of having the National Identification systemm in Tanzania was motivated by various number of factors all aiming for the good well being of the Country out of many reasons stated in Chapter two of this Dissertation.But these positive motive may be destroyed with the few who are having a bad intention first with the project itself and the personal Data of the individuals once they get such opportunity in the absence of sound Data Protection Legal Framework.

5.2 Recommendations

Having observed various Lacuna in the various existing Legislations which attempted in one way or another to provide for Data and Privacy protection regime in Tanzania, it is in the Opinion of the Researcher as follows;

Data Protection Act is to be enacted so as to properly administer matters relating to Data protection and privacy in Tanzania.The Government may start this process in the same manner as done in other enactments which includes other legislative processes before the actual enectment.

This may be done effectively by firstly formulating the Data Protection Policy, where all the purposes and the framework of the Data Protection may be discussed and ultimately helping the future enactment to become comrehensive.Then part of the procedure may be taken care by the Office of the Chief Parliamentary Draftsman (CPD) and the respective Ministry which would be deemed to be the Custodian of the particular Legislation.

Then other legislative processes can be oberseved for example the collection of the opinion from other stakeholders so as to get their views on what they think should be the of paramouncy in the proposed legislation for the Data protection which would suit for the Tanzanian situation. Further, the Government of the United Republic of Tanzania may conteplate on establishing the Supervisory Agency regarding Data Protection which would then act as an Implementor of the newly enacted Data Protection Act.

All issues regarding personal infromation in the National Identification system should be left to NIDA for it the Authority mandated by law to deal with all issues relating to the National Identification and as a custodian of the National population Register.The Data Protection may state for the duty of NIDA regarding the processing of any information extracted from the Databases of NIDA.

REFERENCES

BOOKS

Agre, P. E. and Rotenberg, M., (1998), **"Technology and Privacy: the New Landscape"**, the MIT Press, Cambridge, Massachusetts.

Buergenthal, T. et al, (2004), **"International Human Rights Law in Nutshell",** West Group.

Harris D.J., O'Boyle M. and Warbrick C., (1995), **"Law of the European Convention on Human Rights"**, Butterworth, London.

Jacobs, F.G., & White, C.A., (2006), **"The European Convention on Human Rights",** 4th Ed., Oxford University press, London.

Lloyd, J.I., (2011), **"Information Technology Law",** Oxford University Press, London.

Lloyd, M., (2005), **"The Passport",** Sutton Publishing, Sparkford.

Lyon, D., (2009), **"Identifying Citizens: ID Cards as Surveillance".** Cambridge: Polity Press.

Mambi, A., (2010), **"ICT Law Book",** Mkuki na Nyota, Dar es Salaam.

Solove, D.J., & Rotenberg, M., (2003), **"Information Privacy Law",** Aspen Publishers, New York.

Torpey J., (2000), **"The Invention of the Passport: Surveillance, Citizenship and the State"**, Cambridge University Press, London.

Wacks, R., (1989), **"Personal Information: Privacy and Law",** Clarendon Press.

JOURNALS & ARTICLES

Arora, S., (2008), **"National e-ID card schemes:A European overview",**

Information Security Technical Report 13, 46-53.

Banisar D., (2010), **"Linking ICTs, The Right to Privacy, Freedom of Expression and access to Information"**, *East African Journal of Peace & Human Rights,* Vol.16:1.

Bygrave, L. A., (2002), **"Data Protection Law: Approaching Its Rationale, Logic and Limits"**, Kluwer Law International, The Hague /London/New York.

Bygrave, L. A., (2010), **"Privacy and Data Protection in an International Perspective",** *Scandinavian Studies in Law,* Vol.56.

Gavison, R.,(1980), **" Privacy and the Limits of Law"**, *Yale Law Journal*, Vol.89, No.3.

Greenleaf, G., (2011), **"Global data privacy laws: 40 years of acceleration"**, *Privacy Laws & Business International Report,* Issue 112.

Greenleaf, G., (2010), **"India's National ID System: Danger grows in Privacy Vaccum",** *Computer Law and Security Review 26,* 479-491.

Greenleaf, G., (1998), **"ID Cards inAsia-recent developments",** *Privacy Law & Policy Reporter,* 15; 4 PLR 152.

Joinson, N.A. & Paine C., (2005), **"Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom",** *Journal of Information Science,* JIS-0276, Version 3.0.

Koops, B. J. et al, (2005), **"the Slow Erosion of Privacy",** 12 *Michigan Telecommunications and Technology Law Review* (Vol.12:115).

Lyon, D. (1991), **"British Identity Cards: The Unpalatable Logic of European Membership?"** *The Political Quarterly,* 62: 377–385.

Makulilo, B.A., (2011), **"Registration of Sim Cards in Tanzania: a critical**

evaluation of the Electronic and Postal Communications Act 2010", *Computer and Telecommunication Law Review* 17(2), 48-54.

Makulilo, A.B., **"Privacy and data protection in Africa: a state of the art"**, *International Data Privacy Law*, 2012, Vol. 2, No.3.

Makulilo, A.B., (2012), "**Nigeria's Data Protection bill: Too many surprises",** *Privacy Laws & Business International Report*, No.120, Pp. 25-27.

Nancy Yue Liu., (2008), **"Identifying Legal Concerns in the Biometric Context",** *Journal of International Commercial Law and Technology*, Vol. 3, Issue 1

Nancy Yue Liu., (2011), **"Bio-Privacy: Privacy Regulations and the Challenge of Biometrics",** *Routledge*, 1 edition.

Sobel, R., (2002), **"The Demeaning of Identity and Personhood in National Identification Systems"**, *Harvard Journal of Law & Technology*, Vol. 15, No. 2.

Sullivan C., (2006), **"The United Kingdom Identity Cards Act 2006-Civil or Criminal?** *International Journal of Law and Information Technology*, Vol. 15, No.3.

Ubena J., (2012), "**Privacy-a forgotten right in Tanzania"**, *Journal by Tanganyika Law Society*, Vol. 1 JTLS.

Warren, S. D & Brandeis, L.S., (1890), **"The right to Privacy",** *Harvard Law Review,* Vol.4, No.5.

REPORTS

"An Identity Crisis? A study on the issuance of National Identity Cards in Kenya". A Report by Kenya National Commission on Human Rights.

"**The Registration and Identification of persons in the United Republic of Tanzania"**, Feasibility Study Report of 2006 prepared by Gotham International Limited.

"**The Debate over a National Identification Card",** Report by Century Foundation.

WEBSITES

www.nida.go.tz visited of 15th June, 2013.

www.bailii.org visited on 1st June, 2013.

www.moha.go.tz visited on 10th June, 2013.

www.parliament.go.tz visited on 20th June, 2013.

www.ijlit.oxfordjournals.org visited on 5th June, 2013.

http://www.h-net.org/reviews/showrev.php?id=30999 visited on 31st July,2013.

http://m.dailynews.co.tz/index.php/local-news/15482-muhimbili-employees-get-national-id-cards visited on 20th July, 2013.

http://en.wikipedia.org/wiki/Identity_document#United_Kingdom visted on 26th July, 2013.

http://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf visited on 30th July, 2013.

http://www.google.co.tz/search?q=tanzania+map+showing+bordering+countries&tbm visited on 28th July, 2013.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf visited on 14th July,2013.

http://en.wikipedia.org/wiki/Data_processing visited on 2nd July,2013.

http://www.encyclopedia.com/doc/1O11-datasubject.html visited on 3rd July,2013.

http://bunge.parliament.go.tz/PAMS/docs/3-2002.pdf. Visited on 28th July, 2013.